

HP StorageWorks

Director Element Manager user guide

FW 07.00.00/HAFM SW 08.06.00

Legal and notice information

© Copyright 2001–2005 Hewlett-Packard Development Company, L.P.

© Copyright 2005 McDATA Corp.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Windows is a U.S. registered trademark of Microsoft Corporation.

Printed in USA.

Director Element Manager user guide

Contents

About this guide	11
Intended audience	11
Related documentation	11
Document conventions and symbols	12
Rack stability	13
HP technical support	13
HP-authorized reseller	13
Helpful web sites	14
1 Overview	15
Managing the director	15
Element Manager description	16
Feature keys	19
Using the Element Manager	20
Using dialog boxes	20
Illustrations used in this manual	20
Keyboard navigation	20
Opening the Element Manager	20
Window layout and function	23
Menu bar	24
Product menu	24
Management Style	24
Port	24
FRU	25
Clear System Error Light	25
Enable Unit Beaconing	25
Properties	25
Close	25
Configure menu	25
Identification	25
Operating Parameters	26
Preferred Path	26
Switch Binding	26
Ports	27
Addresses	27
SNMP Agent	27
Open Systems Management Server	27
FICON Management Server	28
Features	28
Date and Time	28
Threshold Alert(s)	28

Open trunking	29
Export Configuration Report	29
Enable Web Server	29
Enable Telnet	29
Logs menu	29
Audit log	29
Event log	29
Hardware log	29
Link Incident log	30
Threshold Alert log	30
Open Trunking log	30
Security log	30
Advanced log: Embedded Port log	30
Advanced log: Switch Fabric log	30
Maintenance menu	30
Port Diagnostics	30
Swap Ports	30
Data collection	31
IPL	31
Set online state	31
Firmware library	31
Enable e-mail notification	31
Enable call home notification	31
Backup & restore configuration	32
Reset configuration	32
Help menu	32
Contents	32
About	32
View tabs	33
View panel	33
Hardware view	33
Director menu	35
Port Card menu	35
CTP Card menu	35
Cooling fan module	35
SBAR Card menu	36
Port Card view	36
Port List view	37
Node List view	38
Performance view	39
FRU List view	42
Status bar	42
Closing the Element Manager	44
Feature permissions	44
Backing up and restoring Element Manager data	47
What is backed up?	48
Backing up to a CD	48

Restoring data from a CD	48
Manual backup procedures	48
2 Monitoring and managing the director	51
Hardware view	51
Identifying FRUs	51
Monitoring director operation	52
Director Status table	52
Status bar status indicator	53
Monitoring hardware operation	53
Obtaining hardware information	56
Displaying FRU information	57
Displaying director information	58
Using menu options	59
Director menu	59
Port Card menu	61
Port menu	61
CTP Card menu	62
SBAR Card menu	62
Port Card view	63
Displaying port information	64
Port Card menu	68
Port menu	69
Port List view	72
Port List view menu options	74
Node List view	75
Node List view menu options	76
Displaying node properties	77
Performance view	79
Performance view menu options	79
Bar graph display	80
Port statistics	80
Class 2 statistics	81
Class 3 statistics	81
Error statistics	81
Operational statistics	83
Traffic statistics with receive and transmit values	83
Using statistics for troubleshooting	83
Button functions	84
FRU List view	84
Port operational states	86
Link incident alerts	87
Threshold alerts	88
3 Configuring the director	89
Configuring identification	90
Configuring management style	91

Configuring operating parameters	91
Configuring switch parameters	91
Switch parameters	92
Domain ID	92
Preferred	92
Insistent	92
Rerouting Delay	93
Domain RSCNs	93
Suppress Zoning RSCNs on zone set activations	94
Director Speed (Director 2/64 only).	94
Configuring fabric parameters	95
Fabric parameters.	95
BB_Credit	95
R_A_TOV	95
E_D_TOV	96
Switch Priority	96
Interop mode.	97
Configuring switch binding	97
Configuring ports	97
Warnings and error messages	101
Menu options	101
Configuring ports (Open Systems management style)	103
Configuring ports (FICON management style)	105
Configuring port addresses (FICON management style)	108
Parameters	108
Configure port addresses procedure	109
Managing stored address configurations (FICON management style).	110
Configuring an SNMP agent	111
Configuring open systems management server	113
Configuring FICON management server	113
Configuring feature key	113
No Feature Key dialog box.	115
Configuring date and time	115
Setting date and time manually	116
Synchronizing date and time.	116
Configuring threshold alerts	117
Creating new alerts	118
Modifying alerts	121
Activating or deactivating alerts	122
Deleting alerts.	122
Configuring open trunking	122
Exporting the configuration report.	122
Enabling Embedded Web Server	123
Enabling Telnet	123
Enabling Alternate Control Prohibited	124
Backing up and restoring configuration data	124

4	Using logs	125
	Using logs	125
	Button functions	125
	Expanding columns	126
	Sorting entries	126
	Audit log	127
	Event log	128
	Hardware log	130
	Link Incident log	132
	Threshold Alert log	133
	Open Trunking Log	133
	Security log	134
	Embedded Port log (Advanced log)	135
	Change button	136
	Switch Fabric log (Advanced log)	137
5	Using maintenance features	139
	Port diagnostics	140
	Swap ports (FICON management style)	140
	Notes	141
	Collect maintenance data	141
	Execute an IPL	141
	Set online state	142
	Manage firmware versions	143
	Enable e-mail notification	143
	Enable call-home notification	144
	Notes	144
	Backup and restore configuration	144
	Backup procedure	145
	Restore procedure	145
	Reset configuration	146
6	Optional features	149
	Preferred Path	150
	Configuring a preferred path	150
	Adding a preferred path	150
	Changing a preferred path	152
	Removing a preferred path	152
	Specifying preferred path example	153
	FICON management server	156
	Installation	156
	Configuring the FICON management server	156
	Open systems management server	158
	Installation	158
	Configuring the open systems management server	159

SANtegrity features.	159
Fabric binding.	159
Online state functions	160
Switch binding	160
Configuring switch binding—overview	160
Notes	160
Enabling and disabling switch binding	161
Editing the switch membership list	162
Enabling and disabling and online state functions.	163
Zoning with switch binding enabled	163
Enterprise fabric mode	164
Features and parameters enabled	164
Fabric Binding	164
Switch Binding	164
Rerouting Delay	164
Domain RSCNs	164
Suppress Zoning RSCNs on Zone Set Activations.	165
Insistent Domain Identification (ID)	165
Open trunking	165
Enabling and configuring Open Trunking	166
Pop-up menu	168
Use Algorithmic Threshold.	168
Threshold %	168
Open Trunking Log	169
A Information and error messages	171
HAFM Application messages	172
Element Manager messages.	185
Index	203
Figures	
1 HAFM appliance and remote client computer configuration (dual Ethernet)	17
2 HAFM application desktop	21
3 Director 2/64 Element Manager window	22
4 Director 2/140 Element Manager window	23
5 Director 2/64 Hardware view	33
6 Director 2/140 Hardware view	34
7 Port Card view	36
8 Port List view	37
9 Node List view	39
10 Performance view	40
11 FRU List view	42
12 Monitoring hardware operation - Director 2/64 Hardware view	54
13 Monitoring hardware operation - Director 2/140 Hardware view	55
14 FRU Properties dialog box	57
15 Port Card FRU Properties dialog box	57
16 Director Properties dialog box	58

17	Configure Date and Time Periodic Synchronization dialog box	60
18	Configure date and time (manually)	60
19	Set Online State dialog box (director is online)	61
20	Set Online State dialog box (director is offline)	61
21	Switchover CTP dialog box	62
22	Port Card view	63
23	Port Properties dialog box	65
24	Port Binding dialog box	70
25	Clear Threshold Alert(s) dialog box	71
26	Port List view	72
27	Node List view	75
28	Node Properties dialog box	77
29	Performance view	79
30	FRU List view	84
31	Configure Identification dialog box	90
32	Configure Switch Parameters dialog box (Director 2/140)	91
33	Configure Fabric Parameters dialog box	95
34	Configure Ports dialog box (Open Systems management style)	103
35	RX BB Credit dialog box	104
36	Configure Ports dialog box (FICON management style)	105
37	RX BB Credit dialog box	105
38	RX BB Credit dialog box	106
39	Prohibited Port connection symbol	108
40	Configure Addresses - "Active" dialog box	109
41	Address Configuration Library dialog box	110
42	Configure SNMP dialog box	112
43	Configure Feature Key dialog box	113
44	New Feature Key dialog box	114
45	Enable Feature Key dialog box	114
46	No Feature Key dialog box	115
47	Configure Date and Time dialog box	116
48	Configure Threshold Alert(s) dialog box	118
49	New Threshold Alerts dialog box - first screen	118
50	New Threshold Alerts dialog box - second screen	119
51	New Threshold Alerts dialog box - third screen	120
52	New Threshold Alerts dialog box - summary screen	120
53	Configure Threshold Alerts dialog box - alert activated	121
54	Export Configuration Report dialog box	123
55	Save dialog box—log windows	126
56	Audit log	127
57	Event log	128
58	Hardware Iwog	130
59	Link Incident Log	132
60	Threshold Alert log	133
61	Security log	134
62	Embedded Port log (FICON style display mode)	135
63	Log Settings dialog box	136

64	Switch Fabric log	137
65	Swap Ports dialog box	140
66	IPL Confirmation dialog box	142
67	Backup and Restore Configuration dialog box.	145
68	Configure Preferred Paths dialog box.	151
69	Add Preferred Path dialog box	152
70	Specifying preferred path for switch 1	154
71	Specifying preferred path for switch 2	154
72	Configure FICON Management Server Parameters dialog box	158
73	Switch Binding State Change dialog box	161
74	Switch Binding Membership List dialog box	162
75	Configure Open Trunking dialog box.	166
76	Open Trunking Log	169

Tables

1	Document conventions	12
2	Operating status—status bar and director Status table	43
3	Permissions required for feature functions	44
4	Port states and indicators	86
5	Event codes	129
6	FRU names	131
7	Data default values	147
8	Available code pages	157
9	HAFM messages.	172
10	Element Manager messages.	185

About this guide

This guide provides information to use when planning to acquire and install one or more of the following Hewlett-Packard (HP) StorageWorks products:

- Director 2/64
- Director 2/140
- High Availability Fabric Manager (HAFM) application

The Director 2/64 is a 64-port director, while the Director 2/140 is a 140-port director. Functions and options available through the Element Managers for these products are nearly identical. When there are differences, this guide will contain notes such as **Director 2/64 only** or **Director 2/140 only**.

Intended audience

This guide is part of a documentation set that supports the Director. This publication is intended for use by configuration and installation planners; however, information is also provided for system administrators, customer engineers, and project managers.

Related documentation

In addition to this guide, please refer Related Documents section of the *HP StorageWorks Director Release Notes*.

For the latest information, documentation, and firmware releases, please visit the HP StorageWorks web site:

<http://h18006.www1.hp.com/storage/saninfrastructure.html>

For information about Fibre Channel standards, visit the Fibre Channel Industry Association web site located at <http://www.fibrechannel.org>.





These and other HP documents can be found on the HP documents web site:

<http://www.docs.hp.com>.

Document conventions and symbols


Table 1 Document conventions

Convention	Element
Medium blue text: Figure 1	Cross-reference links and e-mail addresses
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	<ul style="list-style-type: none">• Key names• Text typed into a GUI element, such as into a box• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
<i>Italics font</i>	Text emphasis
Monospace font	<ul style="list-style-type: none">• File and directory names• System output• Code• Text typed at the command-line
<i>Monospace, italic font</i>	<ul style="list-style-type: none">• Code variables• Command-line variables
Monospace, bold font	Emphasis of file and directory names, system output, code, and text typed at the command line

-  **WARNING!** Indicates that failure to follow directions could result in bodily harm or death.
-  **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.
-  **IMPORTANT:** Provides clarifying information or specific instructions.
-  **NOTE:** Provides additional information.

 **TIP:** Provides helpful hints and shortcuts.

Rack stability

 **WARNING!** To reduce the risk of personal injury or damage to equipment:

- Extend leveling jacks to the floor.
 - Ensure that the full weight of the rack rests on the leveling jacks.
 - Install stabilizing feet on the rack.
 - In multiple-rack installations, secure racks together.
 - Extend only one rack component at a time. Racks may become unstable if more than one component is extended.
-

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support web site:
<http://www.hp.com/support/>.

Collect the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

For continuous quality improvement, calls may be recorded or monitored.

HP strongly recommends that customers sign up online using the Subscriber's choice web site at
<http://www.hp.com/go/e-updates>.

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products by selecting **Business support** and then **Storage** under Product Category.

HP-authorized reseller

For the name of your nearest HP-authorized reseller:

- In the United States, call 1-800-345-1518.
- Elsewhere, visit the HP web site: <http://www.hp.com>. Then click **Contact HP** to find locations and telephone numbers.

Helpful web sites

For third-party product information, see the following HP web sites:

- <http://www.hp.com>
- <http://www.hp.com/go/storage>
- <http://www.hp.com/support/>
- <http://www.docs.hp.com>

1 Overview

This chapter provides an introduction to the HP StorageWorks Director 2/64 and Director 2/140 Element Managers. It is intended as a quick reference for using features available through the main Element Manager window of the High Availability Fabric manager (HAFM) application.

- [Managing the director](#), page 15
- [Element Manager description](#), page 16
- [Using the Element Manager](#), page 20
- [Feature keys](#), page 19
- [Backing up and restoring Element Manager data](#), page 47

Managing the director

You can manage the director through several different interfaces. These interfaces are as follows:

- The Element Manager and HAFM
Installed on a HAFM appliance shipped from the factory. (You access the Element Manager through the HAFM application.)
- Embedded Web Server (EWS) interface
Using a browser-capable PC with an Internet connection to the director, you can monitor and manage the director through the EWS interface embedded in the director firmware. The interface provides a GUI similar to the Element Manager and supports director configuration, statistics monitoring, and basic operation.
To launch the EWS interface:
 1. Enter the director's IP address as the Internet Uniform Resource Locator (URL) into any standard browser.
 2. Enter a user name and password at the login screen. The browser then becomes a management console. (Refer to the Embedded Web Server interface online help or the *HP StorageWorks Embedded Web Server user guide* for details on use.)



NOTE: The default user name for the right to view status and other information is "operator." The default user name for the right to modify configuration data, perform maintenance tasks, or perform other options is "Administrator." The default password for both user names is "password."

- Command Line Interface (CLI).
The CLI allows you to access many HAFM application and Element Manager functions while entering commands during a Telnet session with the switch. The primary purpose of the CLI is to automate management of many switches using scripts. The CLI is not an interactive interface; no checking is done for pre-existing conditions and no prompts display to guide users through tasks. Refer to the *HP StorageWorks CLI reference guide for directors and edge switches* for more information.

- Simple Network Management Protocol (SNMP).

An SNMP agent is implemented through the Element Manager. It allows administrators on SNMP management workstations to access product management information using any standard network management tool. Through the Element Manager, administrators can assign Internet protocol (IP) addresses and corresponding community names for up to six workstations functioning as SNMP trap message recipients. Refer to the *HP StorageWorks SNMP reference guide for directors and edge switches* for more information.

This manual provides details on the Element Manager for the Director 2/64 and Director 2/140 products only. It provides instructions for using the Element Manager through the HAFM application.

Element Manager description

The Element Manager for the director products is a Java-based graphical user interface (GUI) that provides in-depth management, configuration, and monitoring functions for individual directors and their field-replaceable units (FRUs).

The Element Manager provides graphical views of director hardware components and displays of component status. By positioning the mouse pointer on icons, graphics, panels, and other visual elements in these views and clicking the left or right mouse button, you can quickly manage and monitor the director on your network.

The server software for the HAFM and Element Manager comes installed on the HAFM appliance.

You can install the HAFM and Element Manager clients on remote computer systems, as shown in [Figure 1](#) on page 17. For instructions, refer to the section in *HP StorageWorks HA-Fabric Manager user guide* that pertains to the operating system of your computer.

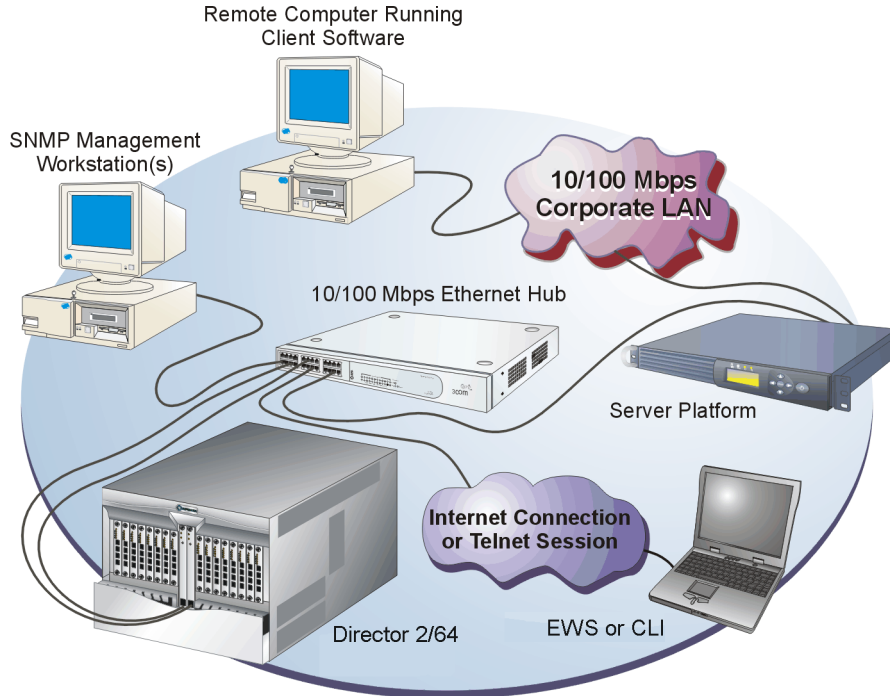



Figure 1 HAFM appliance and remote client computer configuration (dual Ethernet)

Using the Element Manager, you can:

- Back up and restore configuration data.
- Clear the system error indicator.
- Configure extended distance buffering for ports.
- Configure Fibre Channel operating parameters for the director, such as BB_Credit, R_A_TOV, E_D_TOV, preferred domain ID, switch priority, domain RSCNs, preferred and insistent domain ID, director speed (Director 2/64 only), and rerouting delay.
- Configure individual ports with a port name describing the node attached to the port.
- Configure keys for new features.
- Configure link incident (LIN) alerts.
- Configure interoperability mode for multiswitch fabrics.
- Configure Open Trunking if the optional Open Trunking feature is installed.
- Configure preferred paths for interswitch links (ISLs).
- Configure a nickname to display instead of the WWN for the director and for attached node devices.
- Configure Port Binding.

- Configure port address configurations (FICON management style only).
- Configure SNMP trap recipients and community names.
- Configure the FICON and Open Systems Management Server features if optional Open Systems Management Server is installed.
- Configure Switch Binding if optional SANtegrity Binding feature is installed.
- Configure Open Trunking if optional Open Trunking feature is installed.
- Configure the management style between Open Systems and FICON management.
- Configure the director name, location, description, and contact person.
- Configure the data speed for the director (Director 2/64 only) and individual ports.
- Configure threshold alerts for ports.
- Control individual Fibre Channel ports by blocking/unblocking operation, enabling LIN alerts and Port Binding, setting data speeds, and running internal and external loopback diagnostics.
- Display FRU properties such as the FRU name, physical position in the director (chassis slot number), active/failed state, part number, and serial number.
- Display information for individual Fibre Channel ports, such as the port name, port number, Fibre Channel address, operational state, type of port, and login data.
- Display information on nodes attached to ports.
- Display port performance and statistics.
- Display vital product data for the director, such as the system name, description, contact person, location, status, model number, firmware and Engineering Change (EC) level, and manufacturer.
- Enable Alternate Control Prohibited (ACP) to restrict access to FICON director connectivity parameters.
- Enable beaconing for ports and the director unit.
- Enable channel wrap mode (FICON management style only).
- Maintain a port address library (FICON management style only).
- Monitor the operational status of the director and each of its hardware field-replaceable units.
- Perform an initial program load (IPL).
- Perform maintenance tasks for the director including maintaining firmware levels, enabling the call-home feature, accessing the director logs, and collecting data to support failure analysis.
- Reset port operation.
- Run port diagnostics.
- Set the date and time on the director.
- Swap addresses between ports (FICON management style only).

 **NOTE:** You may perform configuration for some features through both the HAFM and the Element Manager. You must also enable Element Manager feature permissions for Administrative, Operator, and Maintenance user levels through the HAFM. When this guide refers to the HAFM for specific tasks, you should see the HAFM online help or the *HP StorageWorks HA-Fabric Manager user guide* for detailed instructions.

Feature keys

Feature keys verify ownership of the Element Manager and optional features that can be purchased for the Element Manager. The feature key, which is encoded with a director's serial number, can only be configured on the director to which it is assigned.

When you purchase additional Element Manager features, you receive a feature key. The feature keys that you are currently using are included in this key.

Here are some important notes about the Element Manager feature key introduced with this release:

- All edge directors that were purchased prior to the release of firmware 06.00.00 will automatically have the Element Manager feature enabled when their firmware is upgraded to version 06.00.00 or later. However, the feature key for the Element Manager will not be added or incorporated into the existing feature key.
- Enabling the **Reset Configuration** option through the Element Manager **Maintenance** menu clears all features that were enabled through the Configure Feature Key dialog box. When you attempt to reinstall features using a feature key assigned for a director prior to the release of 06.00.00, a warning displays that the Element Manager feature key is not installed. You must contact customer support to get a feature key reassigned that includes the Element Manager feature.
- For directors shipped to you with firmware version 06.01.00 or later installed:
 - Feature keys for the Element Manager are activated automatically.
 - Feature keys for additional features you have purchased must be activated through the Configure Feature Key dialog box in the Element Manager. See "[Configuring feature key](#)" on page 113 for more information.


Using the Element Manager

This section provides a general overview of the Element Manager and its functions.

For details on performing specific tasks and using specific dialog boxes, see the appropriate chapters in this manual.

Using dialog boxes

Buttons such as **OK**, **Activate**, **Close** or **Cancel** initiate functions in a dialog box. Click a button to perform its labeled function.

 **NOTE:** There is a difference between the **Close** and **Cancel** buttons. **Close** closes the dialog box and saves the data you entered. **Cancel** cancels the operation and closes the dialog box without saving the information you entered.

Illustrations used in this manual

Figures containing Element Manager screens in this manual are included for illustration purposes only. These illustrations may not match exactly what you see through your HAFM appliance or remote computer running client software. Title bars have been removed from the illustrations, and fields in the illustrations may contain different data than in screens displayed on your system.

Keyboard navigation

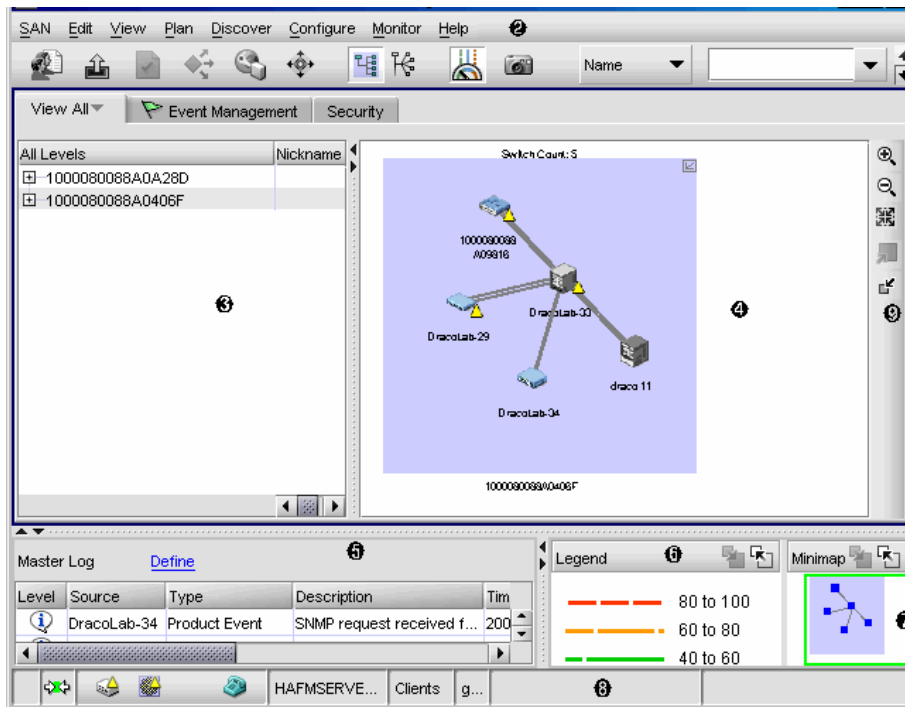
Keyboard navigation is an alternative to mouse navigation. The Element Manager supports standard keyboard navigation and identifies equivalent keystrokes for menu options whenever possible.

Opening the Element Manager

You can access the Element Manager for a director through the HAFM in two different ways:


- In the HAFM application, double-click a director icon on the HAFM Physical/Topology Map, as shown in [Figure 2](#) on page 21.
The Element Manager window displays, showing the Hardware view for the selected director. (See [Figure 3](#) on page 22 or [Figure 4](#) on page 23.)
Or
- Right-click a director icon on the HAFM Physical/Topology Map. (See [Figure 2](#) on page 21.) A pop-up menu displays.
Click **Element Manager**.

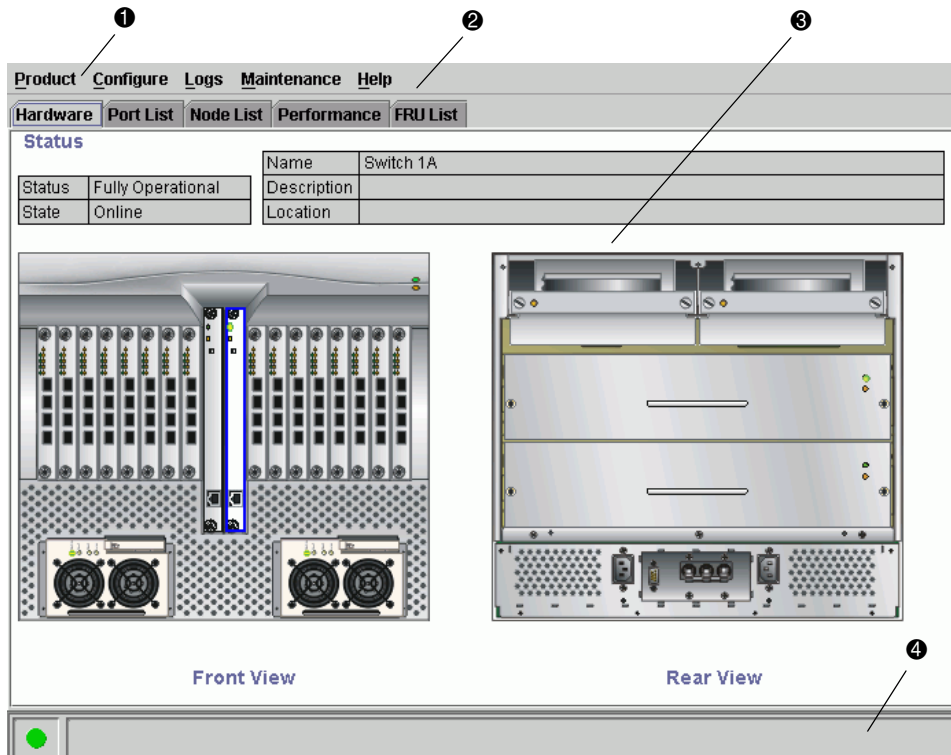
The Element Manager window displays, showing the Hardware view for the selected director. (See [Figure 3](#) on page 22 or [Figure 4](#) on page 23.)



- | | |
|-------------------------|---------------------------------|
| 1 Menu bar | 6 Connection utilization legend |
| 2 Toolbar | 7 Minimap |
| 3 Product list | 8 Status bar |
| 4 Physical/Topology map | 9 Toolbox |
| 5 Master log | |

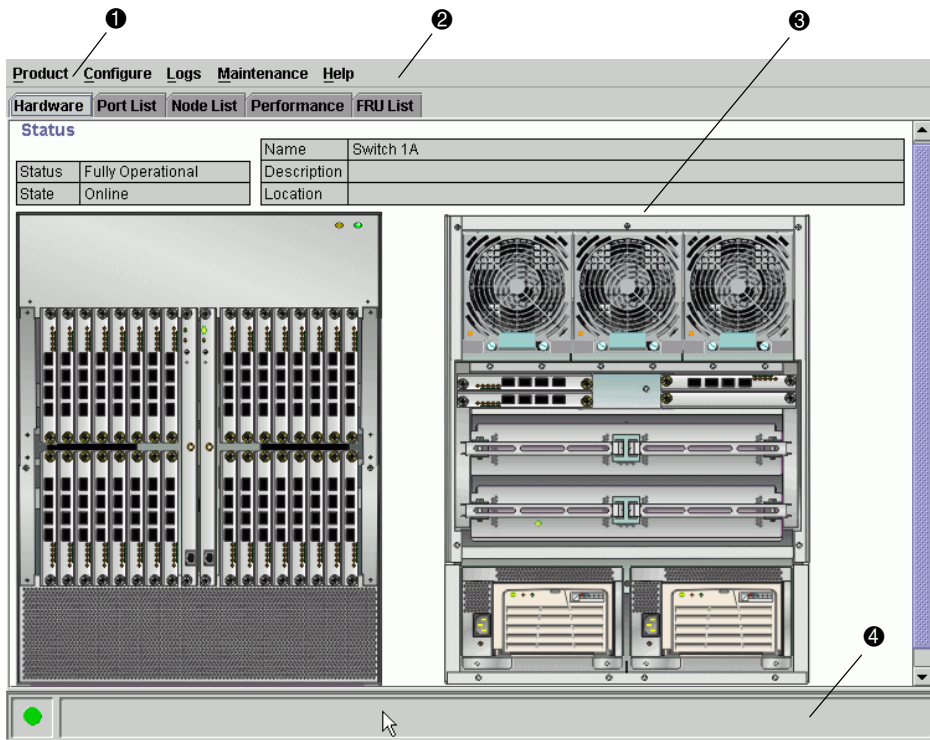
Figure 2 HAFM application desktop

 **NOTE:** Figure 3 displays the Director 2/64 Hardware view and Figure 4 displays the Director 2/140 Hardware view. Other views may display, depending on what you displayed last before closing the Element Manager.



- 1 Menu Bar
- 2 View tabs
- 3 View panel
- 4 Status bar

Figure 3 Director 2/64 Element Manager window



- | | |
|-------------|--------------|
| 1 Menu bar | 3 View panel |
| 2 View tabs | 4 Status bar |

Figure 4 Director 2/140 Element Manager window

NOTE: The HAFM application window is available as a separate window. You can drag the Element Manager window away from the HAFM application window and view both windows on your desktop or minimize one or both of them to icons if desired. You can have a maximum of four Element Manager windows open concurrently.

Window layout and function

The Element Manager window is divided into the following four main areas (See [Figure 3](#) on page 22 or [Figure 4](#).):

- Menu bar
- View tabs
- View panel
- Status bar

The sections that follow describe each of these areas.

Menu bar

The menu bar on the Element Manager window includes the following menus:

- **Product**
- **Configure**
- **Logs**
- **Maintenance**
- **Help**

Click on the name of a menu to display a list of menu options. Click an option to open a dialog box that allows you to perform configuration and maintenance tasks and to view logs.

If a menu option contains a check box, click the box to add a check mark and enable a function. Click a check box containing a check mark to remove the check mark and disable the function.


Product menu

Select the **Product** menu to display the following options.

Management Style

This option provides a secondary menu with option buttons for Open Systems and FICON management styles. These options change some Element Manager dialog boxes and options to allow management of the director in Open Systems or FICON environments.

- **Open Systems**—Click this option button for (non-FICON) Fibre channel environments. Open Systems is the default management style.
- **FICON**—Click this option button when attaching an IBM S/390 Parallel Enterprise or zSeries server to the director and implementing inband director management through a Fibre Connection (FICON) channel. If director firmware level is below 6.0 and the FICON Management Server feature is enabled, the default management style will be FICON. The management style can be changed to Open Systems with the FICON Management Server feature enabled.

 **NOTE:** If firmware versions below 6.0 are installed on the director, you need to take the director offline before changing the management style.

Port

This option provides a secondary port menu only when the Port Card view, Port List view, or Performance view displays in the View panel. To use this menu for a specific port, click a port in the Port Card view, a port's row in the Port List view, or a port's bar graph in the Performance view.

The menu contains options that are identical to those that display when you right-click a port, port row, or port bar graph in those views. For details on these options, see "[Port menu](#)" on page 61.

FRU

Click a serial crossbar (SBAR) card, control processor (CTP) card, port card, power supply module, or cooling fan module in the Hardware view only and then select **Product > FRU** to display a menu of options for the selected FRU. These options are the same menu options that display when you right-click these components in the Hardware view. For details on these options, see the following sections in ["Using menu options"](#) on page 59:

- [Port Card menu](#), page 61
- [CTP Card menu](#), page 62
- [SBAR Card menu](#), page 62

Clear System Error Light

Select this option to turn off the amber system error LED, located below the green power LED on the director front bezel.

Enable Unit Beacons

Click the **Enable Unit Beacons** check box to toggle unit beacons on or off. When the check box has a check mark, unit beacons are on, and the amber system error light on the director front bezel blinks to help users locate the actual unit in an equipment room. When you click the check box to remove the check mark, unit beacons are disabled and the amber LED goes out. You can only enable beacons if there are no system errors (the system error light is off).

Properties

Select this option to display the Director Properties dialog box. This dialog box contains the director name, description, location, and contact person configured through the Configure Identification dialog box. Also included is other product information, as detailed under ["Displaying director information"](#) on page 58. You can also display this dialog box by double-clicking an area in the Hardware view, away from a hardware component.

Close

Select this option to close the Element Manager window.


Configure menu

Select the **Configure** menu to display the following options. For detailed information on using these options, see ["Configuring the director"](#) on page 89.

Identification

Select this option to display the Configure Identification dialog box. Enter the following information in this dialog box:

- **Name**—Enter a product name. Note that you can set this name as the nickname for the director's WWN, using the **Set Name as Nickname** check box. The nickname then displays instead of the WWN in Element Manager views.
- **Description**—Enter a unique product description.
- **Location**—Enter the product's location.
- **Contact**—Enter contact information, either a name, phone number, or e-mail address.

 **NOTE:** This information displays in the identification table at the top of the Hardware view and in the HAFM Physical/Topology Map, if the Physical/Topology Map is configured to display names.

Operating Parameters

This option offers the ability to configure switch and fabric parameters.

- Click **Switch Parameters** to display the Configure Switch Parameters dialog box for setting Fibre Channel operating parameters. In this dialog box, you can set the preferred domain identification (1 to 31) and make it insistent. You can also enable rerouting delay, domain register for state change notifications (RSCNs), and Suppress RSCNs on zone set activation. In addition, you can also set the director data speed (Director 2/64 only). The director must be offline to configure switch speed, preferred domain ID.
- Click **Fabric Parameters** to display the Configure Fabric Parameters dialog box for setting fabric operating parameters. In this dialog box, you can set buffer-to-buffer credit (BB_Credit) from 1 to 60 (default is 16) and the resource allocation time-out value (R_A_TOV) and error detect time-out value (E_D_TOV) in tenth-of-a-second increments.

In addition, you can set the switch priority level (**Principal**, **Default**, or **Never Principal**) and the interoperability modes between **Homogeneous** and **Open Fabric 1.0**. See "[Configuring fabric parameters](#)" on page 95 for more information on configuring these parameters for the director. The director must be offline to configure any fabric operating parameter.

Preferred Path

Select this option to configure an ISL between switches and directors. The ISL will consist of the source port of the switch being configured, the exit port of the same switch, and the domain ID of the destination switch. Each switch must be configured for its part of the desired path for optimal performance. You may need to configure preferred paths for all switches along the desired path for proper multi-hop preferred path operation. For more details about this feature, see "[Exporting the configuration report](#)" on page 122.

Switch Binding

This option has two suboptions: **Change State** and **Edit Membership List**.

- **Change State**—Displays the Switch Binding State Change dialog box where you can activate Switch Binding according to a specific connection policy (Restrict E_Ports, Restrict F_Ports, or Restrict All Ports).
- **Edit Membership List**—Allows you to create a list of switches and devices that you want to allow exclusively to attach to director ports. Switch Binding is an optional feature that requires the SANtegrity Binding feature key. The feature can be installed through the Configure Feature Key dialog box. For more information, see "[Configuring feature key](#)" on page 113 and "[SANtegrity features](#)" on page 159.


Ports

Select this option to display the Configure Ports dialog box. This dialog box has different functions for FICON management style and Open Systems management style.

- **FICON management style**—Use the dialog box to enable extended distance buffering for 10 to 100 km, link incident (LIN) alerts, and Port Binding for each port.
- **Open Systems management style**—For each port you can provide a name, block or unblock operation, configure extended distance buffering for 10 to 100 km, enable LIN alerts for each port, define a type (G, F, and E), set the speed, enable Port Binding, and enter a WWN or nickname.

 **NOTE:** Ports are automatically configured as G_Ports if no device is connected, F_Ports if a device is connected, and E_Ports if a director is connected.

In both styles, you can enable the rerouting delay feature, and for the Director 2/64 only, you can set the director data speed.

 **NOTE:** Note that your director model and firmware may not allow variable data speeds.

Addresses

FICON management style only. Select one of the following options:

- **Active Addresses**—Displays the Configure-Addresses — “Active” dialog box. Use this dialog box to configure a name, blocked or unblocked state, and prohibited and allowed connection attributes for a port.
- **Stored Addresses**—Displays the Address Configuration Library. Use this dialog box to activate, modify, delete, and modify existing address configurations created through the Active Addresses dialog box.

SNMP Agent

Select this option to display the Configure SNMP dialog box. Use this dialog box to configure network addresses and community names for up to six SNMP trap recipients. Also authorize write permissions to enable SNMP management stations to modify writable MIB variables. In addition, you can enable authorization traps to be sent to management stations when unauthorized stations request access to director SNMP data.

Open Systems Management Server

This option only displays if the Open Systems Management Server inband management feature was enabled through the Configure Feature Key dialog box. (See “[Configuring feature key](#)” on page 113 for more information.) You can select the following check boxes from this option:

- **Enable Open Systems Management Server**—Select this check box to display a check mark enable the Open Systems Management Server.

- **Host Control Prohibited**—Select this check box to display a check mark and prohibit the host management program from changing configuration and connectivity parameters on the director. In this case, the host program has read-only access to configuration and connectivity parameters.

FICON Management Server

This option only displays if the FICON Management Server inband management feature was enabled through the Configure Feature Key dialog box. (See “[Configuring feature key](#)” on page 113 for more information.) You can select the following suboptions:

- **Enable FICON Management Server**—Select the check box to display a check mark and enable the FICON Management Server.
- **Parameters**—Select this option to display the Configure FICON Management Server dialog box. Use this dialog box to perform the following tasks:
 - Allow or prohibit director clock alert mode.
 - Allow or prohibit programmed offline state control.
 - Select a code page from the **Code Page** drop-down list.

For details, see “[FICON management server](#)” on page 156.

Features

This option displays the Configure Feature Key dialog box. Use this dialog box to enter a feature key to enable optional features that you have purchased for the director. (See “[Configuring feature key](#)” on page 113 for more information.)

Date and Time

Select this option to display the Configure Date and Time dialog box. Use this option to set the current date and time in the director. When the **Periodic Date/Time Synchronization** check box is checked, the **Date and Time** fields are grayed out (disabled), and the HAFM appliance’s date and time periodically synchronizes the director date and time. If the **Periodic Date/Time Synchronization** check box is not checked, you can set the date and time in the dialog box fields manually.

Threshold Alert(s)

Select this option to configure threshold alerts for ports. A threshold alert notifies users when the transmit (Tx) or receive (Rx) throughput reaches specified values for specific director ports or port types (E_Ports or F_Ports). Using this option, you can configure:

- A name for the alert.
- A threshold type for the alert (Rx, Tx, or both).
- Active or inactive state of the alert.
- Threshold criteria. This includes configuring the threshold as the percent of port traffic capacity utilized (**% utilization**). You must also configure the time interval during which the throughput is measured and the maximum cumulative time that the throughput percentage threshold can be exceeded during this time interval before an alert is generated.

Open trunking

Select this option to enable the optional Open Trunking feature. This feature monitors the average data rates of all traffic flows on ISLs (from a receive port to a target domain), and periodically adjusts routing tables to reroute data flows from congested links to lightly loaded links to optimize bandwidth use. The feature can be installed through the Configure Feature Key dialog box. See ["Configuring feature key"](#) on page 113 and ["Open trunking"](#) on page 165 for more information.

Export Configuration Report

Select this option to display the Export Configuration Report dialog box, which enables you to specify a file name in which to save an ASCII text file containing all current user-definable configuration options in a printable format. Note that this file cannot be read back into the Element Manager in order to set configuration parameters.

Enable Web Server

Select this option to place a check mark in the check box to enable the EWS interface on the director. Click the option again to remove the check mark and disable the EWS interface. When disabled, users at remote computers running the client software cannot access the EWS interface.

Enable Telnet

Select this option to place a check mark in the check box to enable Telnet access to the director. Click the option again to remove the check mark and disable telnet access. When disabled, users at remote computers running client software cannot access the director through Telnet to use the command line interface (CLI) or perform other tasks.

Logs menu

Select the **Logs** menu to display the following options. For detailed information on using these dialog boxes, see ["Using logs"](#) on page 125.

Audit log

This log provides a record of all configuration changes made on the director. Each entry displays the date and time of the change, a description of the change, the source of the change (such as the HAFM appliance or SNMP management station), and an identifier for the source, such as the IP address of the HAFM appliance or SNMP management station. For more details on this log, see ["Audit log"](#) on page 127.

Event log

Select this option to display the director Event Log. This log provides a record of significant events that have occurred on the director, such as hardware failures, degraded operation, and port problems. Each entry includes the date and time of the event, a reason code for the event, the severity level, a brief description, and up to 32 bytes of supplementary event data. For more information, refer to the HP StorageWorks Director 2/64 service manual for the Director 2/64 and the HP StorageWorks Director 2/140 service manual for the Director 2/140. For more details on this log, see ["Event log"](#) on page 128.

Hardware log

This log displays information on FRUs inserted and removed from the director. Each log entry includes the name of the FRU inserted or removed, the slot position relative to identical FRUs

installed, whether the FRU was inserted or removed, the FRU part number and serial number, and the date and time the FRU was inserted or removed. For more details on this log, see "[Hardware log](#)" on page 130.

Link Incident log

The link incident (LIN) log displays the most recent incidents with their date and time, port number, and description of the incident. A link incident can be one of several conditions detected on a fiber optic link. For a list of events that may cause a link incident to be written to the log, see "[Link Incident log](#)" on page 132.

Threshold Alert log

This log provides notifications of threshold alerts. Besides the date and time that the alert occurred, it also displays information that was configured through the **Configure Threshold Alert(s)** option under the **Configure** menu. This includes the alert name, port for which the alert is configured, the type of alert (transmit throughput, receive throughput, or both), threshold utilization of traffic capacity, minutes for which the threshold was configured, and the configured time interval for the threshold. For more details on this log, see "[Threshold Alert log](#)" on page 133.

Open Trunking log

This log provides details on flow rerouting that is occurring through director ports. See "[Open Trunking Log](#)" on page 169 for details.

Security log

The Security log includes information about security events. For more details on this log, see "[Security log](#)" on page 128.

Advanced log: Embedded Port log

This log provides a detailed history log of all traffic passing through the embedded port. For more details on this log, see "[Embedded Port log \(Advanced log\)](#)" on page 135.

Advanced log: Switch Fabric log

This log includes information about switches in a fabric. For more details on this log, see "[Switch Fabric log \(Advanced log\)](#)" on page 137.

Maintenance menu

Select the **Maintenance** menu to display the following options. For detailed information on using these dialog boxes, see "[Collect maintenance data](#)" on page 141.

Port Diagnostics

This option displays the **Port Diagnostics** dialog box. Use this dialog box to run internal and external loopback tests on ports. For instructions, refer to the HP StorageWorks Director 2/64 service manual for the Director 2/64 and the HP StorageWorks Director 2/140 service manual for the Director 2/140.

Swap Ports

FICON management style only—Displays the Swap Ports dialog box. Use this dialog box to swap one port address for another.

Data collection

This option displays the Save Data Collection dialog box. Use this dialog box to collect maintenance data into a file. This file is used by support personnel to diagnose system problems. For instructions, refer to the *HP StorageWorks Director 2/64 service manual* for the Director 2/64 and the *HP StorageWorks Director 2/140 service manual* for the Director 2/140.

IPL

Select this option to initiate an initial program load on the director. A dialog box displays to allow you to confirm the IPL. Note that an IPL does not affect any configuration settings done through the Element Manager. Port operation is not interrupted during the IPL.

For instructions, refer to the *HP StorageWorks Director 2/64 service manual* for the Director 2/64 and the *HP StorageWorks Director 2/140 service manual* for the Director 2/140.

Set online state

Select this option to display the Set Online State dialog box. Use this dialog box to change the online state of the director to offline or online.

Firmware library

Select this option to display the Firmware Library dialog box. This dialog box displays all firmware versions currently installed on the HAFM appliance that can be downloaded to directors. Use this dialog box to add a new firmware version to the HAFM appliance's hard disk, modify the description displayed for an existing version, delete a version from the PC, or download (send) a version for operation on a director.

For additional information on using this option, refer to the *HP StorageWorks Director 2/64 service manual* for the Director 2/64 or the *HP StorageWorks Director 2/140 service manual* for the Director 2/140.

Enable e-mail notification

The Simple Mail Transfer Protocol (SMTP) server, e-mail recipient addresses, and e-mail notification are configured in the HAFM application (not in the director's Element Manager) for all products. However, the **E-Mail Notification** option on the Element Manager's **Maintenance** menu must be enabled (checked) for e-mail notification to occur for the specific director.

The default setting for the **Enable E-Mail Notification** option is enabled (checked). To disable the option, select **Maintenance > Enable E-Mail Notification** to clear the check box.

For additional information on using this option, see ["Enable e-mail notification"](#) on page 143.

Enable call home notification

Select **Maintenance > Enable Call Home Notification** to enable the call-home function for the director.

The parameters of the call-home feature are configured in Windows®. For instructions, refer to the *HP StorageWorks HA-Fabric Manager Appliance installation guide*.

Backup & restore configuration

Select this option to save the product configuration stored on the director to the HAFM appliance hard disk or to restore the configuration data from the HAFM appliance. Only a single copy of the configuration is kept on the appliance.

This backup is primarily for single-CTP systems, where a backup is needed to restore the configuration data to a replacement CTP card. You cannot modify the location or the file name of the saved configuration.

For additional information on using this option, see ["Backing up and restoring configuration data"](#) on page 124.



NOTE: You can only restore the configuration to a director with the same IP address.

Reset configuration

Select this option to reset all director configuration data back to the factory defaults. When you select this option, a confirmation dialog box displays with a warning. For additional information on using this option, see ["Reset configuration"](#) on page 146.

△ **CAUTION:** This operation resets all configuration including any optional features that have been installed. You will need to re-enter your feature key to enable all optional features after resetting the configuration.

Help menu

Select the **Help** menu to display the following options.

Contents

Select this option to display the Help window. The Help window contains **Contents**, **Index**, and **Search** buttons and hypertext-linked items to help you quickly navigate through information. Use the forward (➤) and back (➤) buttons to scroll forward and backward through the displayed Help frames. Exit the Help feature at any time by clicking the Close icon at the top of the Help window.

About

Select this option to display the version number for the Element and copyright information.

View tabs

Select one of the following view tabs across the top of the Element Manager window to display related information and menus in the View panel:

- **Hardware**
- **Port List**
- **Node List**
- **Performance**
- **FRU List**

View panel

Views selected from the view tabs display under the tabs in the View panel. For detailed information on using these views, see ["Monitoring and managing the director"](#) on page 51.

Hardware view

The Hardware view displays the current hardware components and field replaceable units (FRUs) installed in the director. Menu options in this view allow you to control component operation. Menu options, as well as visual status indicators, allow you to monitor component status. See [Figure 5](#) on page 33 for an example of the Director 2/64 Hardware view and [Figure 6](#) on page 34 for an example of the Director 2/140 Hardware view.

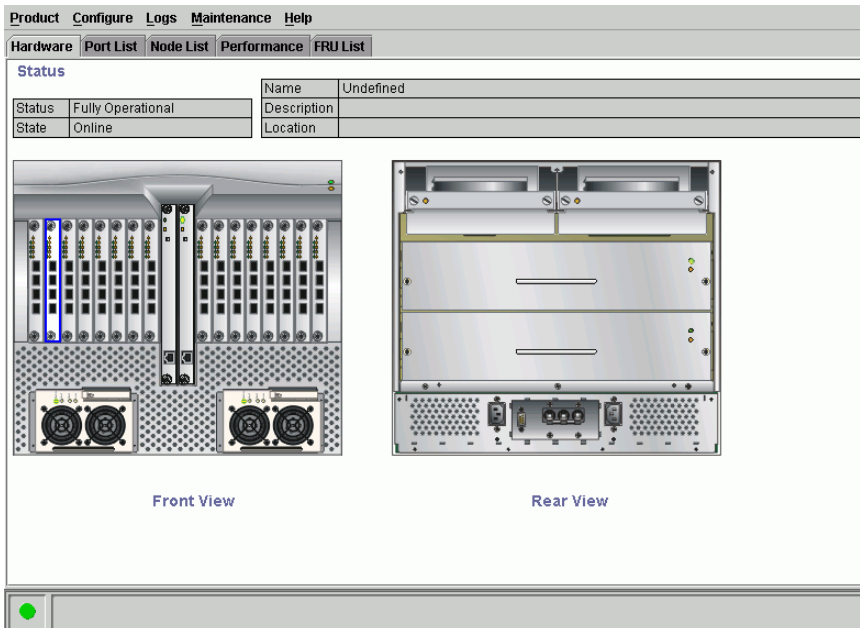


Figure 5 Director 2/64 Hardware view

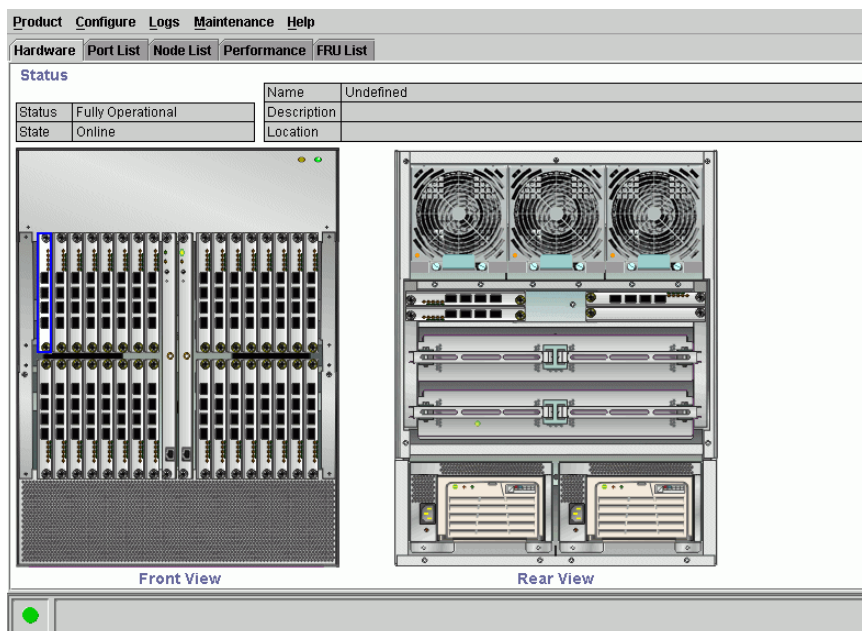


Figure 6 Director 2/140 Hardware view

In the Hardware view, colored indicators reflect the status of actual LEDs on the director FRUs. The status bar displays a symbol to represent the most degraded status currently reported by any of the director FRUs. For example, for a port failure, indicated by a blinking red and yellow diamond on a port, a yellow triangle displays on the status bar to indicate a degraded condition. However, if a blinking red and yellow diamond displays over both SBAR cards, the status bar displays a red and yellow diamond, which indicates a failure requiring immediate attention. For an explanation of the different status symbols and the reasons they display in the Hardware view or Port List view, see to ["Monitoring hardware operation"](#) on page 53.

Double-click the power supply, CTP card, cooling fan module, or SBAR card to display an FRU Properties dialog box containing detailed information on the hardware component. Double-click the director, away from an FRU, to display the Director Properties dialog box.

For details on navigating and monitoring via the Hardware view, see ["Monitoring and managing the director"](#) on page 51.

Director menu

Right-click the graphic away from an FRU to display the Director Properties dialog box. Right-click the graphic to display the following options:

- **Properties**
- **Enable Unit Beaconing**
- **Clear System Error Light**
- **IPL**
- **Date/Time**
- **Set Online State**

For details on menu options, see ["Director menu"](#) on page 59.

For details on navigating and monitoring via the Hardware view, see ["Monitoring and managing the director"](#) on page 51.

Port Card menu

Double-click a port card to display the Port Card view. For details on this view, see ["Port Card view"](#) on page 63. Right-click a port card to display the following options:

- **Open Port Card View**
- **FRU Properties**
- **Enable Port Card Beaconing**
- **Block All Ports**
- **Unblock All Ports**
- **Diagnostics**

These options are also available when you click the port card and select **Product > FRU** on the menu bar.

CTP Card menu

Double-click a CTP card to display the Properties dialog box for the card. Right-click a CTP card to display the following options (for details, see ["CTP Card menu"](#) on page 62):

- **FRU Properties**
- **Enable Card Beaconing**
- **Switchover**

These options are also available when you click the CTP card and select **Product > FRU** on the menu bar.

Cooling fan module

Double-click a fan module on the Rear view to display the FRU Properties dialog box for the module.

This option is also available when you click the fan module and select **Product > FRU** on the menu bar.

SBAR Card menu

Double-click a serial crossbar (SBAR) to display its FRU Properties dialog box. Right-click an SBAR card to display the following options: For details see “[SBAR Card menu](#)” on page 62.

- **FRU Properties**
- **Enable Card Beacons**
- **Switchover**

These options are also available when you click the SBAR card and select **Product > FRU** on the menu bar.

Port Card view

To display the Port Card view for a port, as shown in [Figure 7](#) on page 36:

- Double-click a port card in the Hardware view.
Or
- Right-click a port card and click **Open Port Card View**.

The Port Card view displays, as shown in [Figure 7](#).

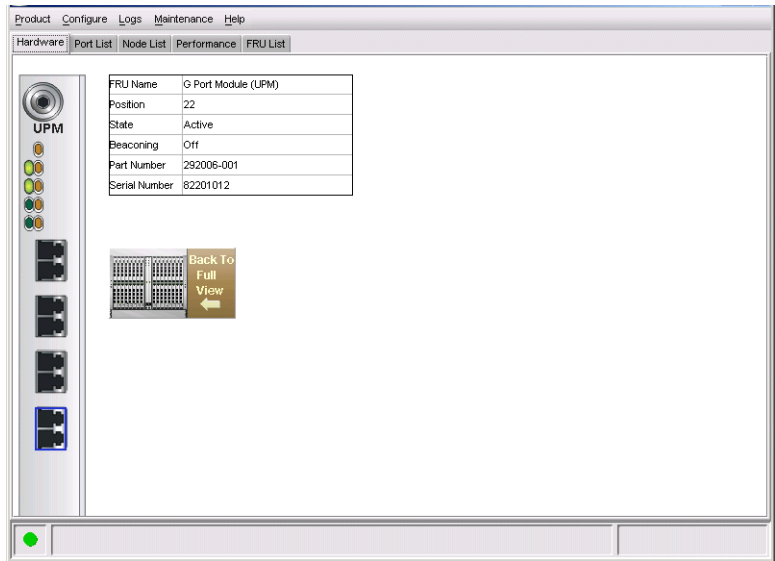


Figure 7 Port Card view

In this expanded view of the port card, you can:

- Determine the port card status by viewing the amber LED at the top of the card. Identify the FRU name, position, operating state, beacons state, and part number of the port from the table shown in this view.
- Determine port status and operation by the status symbols that display next to the port connectors and simulated LED indicators above the connectors.

- Right-click the port card to display a pop-up menu with these options: **Block All Ports**, **Unblock All Ports**, and **Diagnostics**.
- Right-click the port connector to display a menu with these options: **Port Properties**, **Node Properties**, **Port Technology**, **Block Port**, **Enable Beaconing**, **Diagnostics**, **Channel Wrap** (FICON management style only), **Swap Ports** (FICON management style only), **Clear Link Incident Alert(s)**, **Reset Port**, **Port Binding**, and **Clear Threshold Alert(s)**.

These options also display when you click a port connector and select **Product > Port**.

- Double-click a port connector to display the Port Properties dialog box.
- Return to the Hardware view by clicking **Back to Full View**.

See "Port Card view" on page 63 for detailed information on this view.

Port List view

To display the Port List view, click the **Port List** view tab. A table, as shown in Figure 8, displays in the View panel. This table includes the port number, port name, port address (FICON management style only), the block/unblock configuration, operating state, port type of the selected port.

Product Configure Logs Maintenance Help							
Hardware Port List Node List Performance FRU List							
Port #	Name	Block Config	State	Type	Operating Speed	Alert	
0		Unblocked	Offline	G_Port	1 Gig		
1		Unblocked	Online	F_Port	1 Gig		
2		Unblocked	Online	F_Port	1 Gig		
3		Unblocked	Online	F_Port	1 Gig		
4		Unblocked	Offline	G_Port	1 Gig		
5		Unblocked	Online	F_Port	1 Gig		
6		Unblocked	Online	F_Port	1 Gig		
7		Unblocked	Online	F_Port	1 Gig		
8		Unblocked	Offline	G_Port	1 Gig		
9		Unblocked	Online	F_Port	1 Gig		
10		Unblocked	Online	F_Port	1 Gig		
11		Unblocked	Online	F_Port	1 Gig		
12		Unblocked	Offline	G_Port	1 Gig		
13		Unblocked	Online	F_Port	1 Gig		
14		Unblocked	Online	F_Port	1 Gig		
15		Unblocked	Online	F_Port	1 Gig		
16		Unblocked	Offline	G_Port	1 Gig		
17		Unblocked	Online	F_Port	1 Gig		
18		Unblocked	Online	F_Port	1 Gig		
19		Unblocked	Online	F_Port	1 Gig		
20		Unblocked	Offline	G_Port	1 Gig		
21		Unblocked	Online	F_Port	1 Gig		
22		Unblocked	Online	F_Port	1 Gig		
23		Unblocked	Online	F_Port	1 Gig		

Figure 8 Port List view

The Port List view displays information about all ports installed in the director. All data is dynamic and updates automatically. Double-click any row in this view to display the Port Properties dialog box for the port.

Right-click a port row to display the same menu options that display when you right-click a port in the Port Card view or a port's bar graph in the Performance view. These include:

- **Port Properties**
- **Node Properties**
- **Port Technology**
- **Block Port**
- **Enable Beacons**
- **Diagnostics**
- **Channel Wrap** (FICON management style only)
- **Swap Ports** (FICON management style only)
- **Clear Link Incident Alert(s)**
- **Reset Port**
- **Port Binding**
- **Clear Threshold Alert(s)**

These options also display when you click a port row and select **Product > Port**.

For details on these menu options, see "[Port menu](#)" on page 69.

For details on navigating and monitoring using the Port List view, see "[Port List view](#)" on page 72.

Node List view

To display the Node List view, click the **Node List** view tab. A table, as shown in [Figure 9](#) on page 39, displays in the View panel. This table provides information about all node attachments or N_Ports that have logged in to existing F_Ports on the director. Only N_Ports display in the Node List view after nodes have logged in to the fabric.

The columns that display in the table include: port number where the node is attached, the port's address, WWN of the attached node's port, unit type, and BB_Credit used by the attached node.

To display the Node Properties dialog box for a port, double-click the port row.

To display the following menu options for a port, right-click the port row:

- **Node Properties**—Displays the Node Properties dialog box.
- **Port Properties**—Displays the Port Properties dialog box.
- **Define Nickname**—Displays the Define Nickname dialog box, where you can define a nickname to display for the attached device instead of the device's eight-byte WWN.

- **Display options**—Allows you to display attached devices listed under the **Port WWN** column in the Node List view by the device's nickname configured through the **Define Nickname** option or the device's WWN.

Port #	Address	Port WWN	Unit Type	BB_Credit
90	635E13	Digital Equipment -50:00:1F:E1:00:14:2C:C4	Reserved	2
94	636213	Digital Equipment -50:00:1F:E1:00:14:2C:C1	Reserved	2

Figure 9 Node List view

These options also display when you click a port row and select **Product > Port**.

For details on navigating and monitoring via the Node List view, see "[Node List view](#)" on page 75.

Performance view

To display the Performance view, click the **Performance** tab. The Performance view, as shown in [Figure 10](#) on page 40, displays. This view provides a graphical display of performance for all ports. The top portion of the Performance view displays bar graphs that show the level of transmit/receive activity for each port. (Use the scroll bar to view bar graphs for all the ports.) The information in this view updates every five seconds. Each bar graph also shows the percentage link utilization for the port. A red arrow marks the highest utilization level reached since the Performance view was opened. If the system detects activity on a port, it represents minimal activity with at least one bar.

When an end device (node) is logged in to a port, moving the mouse pointer over the port's bar graph in the Performance view highlights the graph and displays a message with the WWN of the connected node. If the connected node has more than one port, this is the WWN of the specific port on the node.

When a port is functioning as an expansion port (E_Port), the message is E_Port. When a port is not logged into an end-device (not functioning as an F_Port) or to another director (not functioning as an E_Port), the message is the port's current online state.

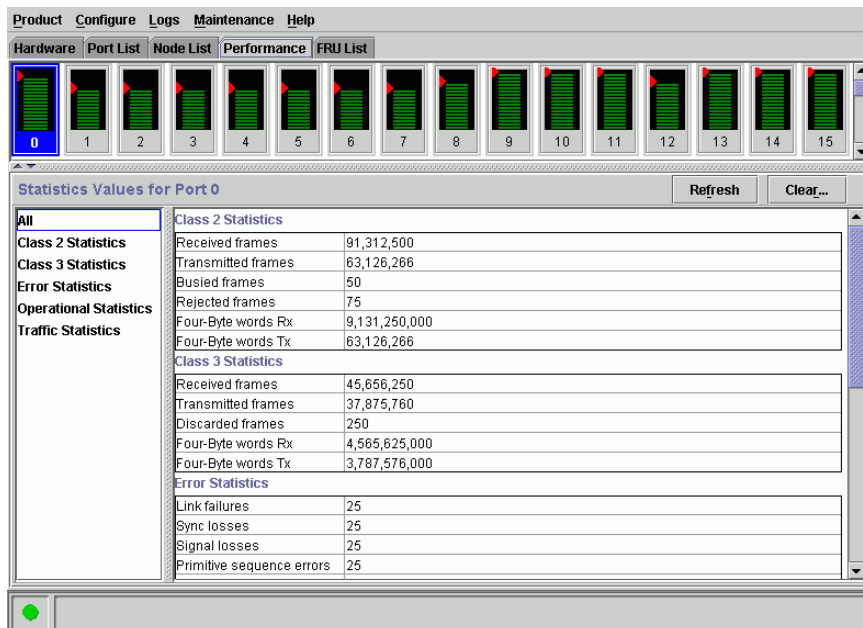


Figure 10 Performance view

To display a menu of port-related actions, right-click a bar graph. The options available on this menu are the same as those that are available when you right-click a port in the Port Card view or right-click a row in the Port List view. These include:

- **Port Properties**
- **Node Properties**
- **Port Technology**
- **Block Port**
- **Enable Beaconsing**
- **Diagnostics**
- **Channel Wrap** (FICON management style only)
- **Swap Ports** (FICON management style only)
- **Clear Link Incident Alert(s)**
- **Reset Port**
- **Port Binding**
- **Clear Threshold Alert(s)**

These options also display when you click a port row and select **Product > Port**.

For details on port menu options, see "[Port menu](#)" on page 69.

The bottom portion of the Performance view displays cumulative statistical information for the port selected in the bar graph. Values are displayed for the following categories:

- **Class 2 Statistics**
- **Class 3 Statistics**
- **Error Statistics**
- **Operational Statistics**
- **Traffic Statistics**

Select a category in the left frame of the statistics area to display only statistics in that category, or click **All** to display values for all categories.

To update the display with current data from the port, click **Refresh**.

To clear all counters:

1. Click **Clear** to display the Clear Port Statistics dialog box.
2. Click the appropriate option button to:
 - Reset all counters to zero on the selected port.
Or
 - Reset all counters on all ports on the director.
3. Click **OK**.



NOTE: Clearing the counters clears the statistics for all users.

For more information about the Performance view, including statistics descriptions, see "[Performance view](#)" on page 79.

FRU List view

To display the FRU List view, click the **FRU List** view tab. A table, as shown in [Figure 11](#), displays in the View panel. This table includes information about each FRU installed in the director. All data is dynamic and updates automatically.

FRU	Position	Status	Part Number	Serial Number
Backplane	0	Active	316143-001	T2374878
Control Processor (CTP)	0	Active	254136-001	82372257
Control Processor (CTP)	1	Backup	316145-001	82372253
Serial Crossbar (SBAR)	0	Active	316144-001	82380004
Serial Crossbar (SBAR)	1	Backup	316144-001	82202000
Cooling Fan Module	0	Active		
Cooling Fan Module	1	Active		
Cooling Fan Module	2	Active		
Power Supply Module	0	Active	316141-001	52074128
Power Supply Module	1	Active	316141-001	52074155
G Port Module (UPM)	0	Active	292006-001	82301030
G Port Module (UPM)	1	Active	292006-001	82300772
G Port Module (UPM)	2	Active	292006-001	32473480
G Port Module (UPM)	3	Active	292006-001	32473357
G Port Module (UPM)	4	Active	292006-001	32473600
G Port Module (UPM)	5	Active	292006-001	32473349
G Port Module (UPM)	6	Active	292006-001	82301895
G Port Module (UPM)	7	Active	292006-001	82250602
G Port Module (UPM)	8	Active	292006-001	32320072
G Port Module (UPM)	9	Active	292006-001	82342010
G Port Module (UPM)	10	Active	292006-001	32473586
G Port Module (UPM)	11	Active	292006-001	32472064
G Port Module (UPM)	12	Active	292006-001	82221858
G Port Module (UPM)	14	Active	292006-001	82270485
G Port Module (UPM)	15	Active	292006-001	82300773
G Port Module (UPM)	16	Active	292006-001	82321780
G Port Module (UPM)	17	Active	292006-001	82230786
G Port Module (UPM)	18	Active	292006-001	82341759
G Port Module (UPM)	19	Active	292006-001	32473305

Figure 11 FRU List view

To display a Properties dialog box for an FRU, click on the FRU row and then select **Product > FRU > FRU Properties**.

For details on navigating and monitoring via the FRU List view, see [“FRU List view”](#) on page 84.





Status bar

The status bar is located along the bottom of the Element Manager window. (See [Figure 3](#) on page 22 or [Figure 4](#) on page 23.) Then status bar includes a symbol that displays on the left side of the bar and messages that display in the panel to the right of the symbol. The symbol indicates the current operating status of the director, and the messages provide descriptions of menu options as you move the mouse pointer over the options under the menu bar.

See [Table 2](#) on page 43 for the meaning of these status symbols and of the corresponding alert text that displays in the Status table at the top of the Hardware view in the main panel.

If a gray square displays in the status bar (no Ethernet connection), a reason for the status displays in the Status table at the top of the Hardware view. See “[Director Status table](#)” on page 52 for details. See [Table 2](#) for the meanings of status symbols that display in Element Manager views.

Table 2 Operating status—status bar and director Status table

Symbol	Status bar	Director Status table text	Description
	Green Circle	Fully Operational	All components and installed ports are operational; no failures.
	Yellow Triangle	Redundant Failure	A redundant component has failed, such as a power supply, and the backup component has taken over operation.
		Minor Failure	A failure occurred which has decreased the director operational ability. Normal switching operations are not affected. One or more Port cards failed, but at least one Port card is still operational. A fan has failed or is not rotating sufficiently. One of two CTP cards failed. One of two SBAR cards failed.
	Red and Yellow Diamond	NOT OPERATIONAL	A critical failure prevents the director from performing fundamental switching operations. All fans fail. Both SBAR cards fail. All installed Port cards fail.
	Gray Square	Never Connected Link Timeout Protocol Mismatch Duplicate Session Unknown Network Address Incorrect Product Type	Director status is unknown. This occurs if the Ethernet network connection between the HAFM appliance and the director cannot be established or if the CTP fails. See “ Director Status table ” on page 52 for details on the status table text.

Closing the Element Manager

To close the Element Manager, do one of the following:

- Select **Product > Close** on the menu bar.
- Double-click the icon at the top left corner of the Element Manager window, or click the icon and click **Close** on the menu that displays.

Feature permissions

The system administrator can allow users access to specific functions of Element Manager features through HAFM.

The *HP StorageWorks HA-Fabric Manager user guide* provides detailed instructions for assigning permissions.

There are three permission levels that can be assigned to specific users:

- Device Administration
- Device Operation
- Device Maintenance

By default, all users have read-only rights, which allow viewing but not modifying data or configurations. You can enable each of the permission levels as either read-only or read/write for specific users. Users that are assigned a permission level that is required for a specific feature must also be given read/write access to modify any data through the feature. For example, to clear the Audit Log, a user must be assigned Device Administration permission, as well as read/write access. If a user is assigned Device Administration permission, but read-only access, that user can only view the Audit Log.

Table 3 itemizes specific functions available to Element Manager users who have been assigned Device Administration, Device Operation, and Device Maintenance permissions. The user must also be assigned read/write access to perform functions that modify data or configurations. If a user does not have permission to perform a specific operation, a not-authorized error box displays when the operation is attempted.

Table 3 Permissions required for feature functions

Element Manager rights	Device administration	Device operation	Device maintenance	Security administration
Allow or prohibit Matrix, Active (FICON style only)	X	X		
Allow or prohibit Matrix, Stored (FICON style only)	X	X		
Enable Alternative Control Prohibit	X			
Backup and Restore Configuration	X	X	X	

Table 3 Permissions required for feature functions (continued)

Element Manager rights	Device administration	Device operation	Device maintenance	Security administration
Channel Wrap (FICON management style)	X		X	
Clear Audit Log	X			
Clear Event Log			X	
Clear Hardware Log	X		X	
Clear LIN Alert	X	X	X	
Clear LIN Log	X			
Clear System Error Light			X	
Clear Threshold Alerts	X			
Clear Threshold Event Log	X			
Configure Addresses – “Active” (FICON management style)	X	X		
Configure Addresses – “Stored” (FICON management style)	X			
Configure Date/Time	X	X	X	
Configure Feature Key	X			
Configure Identification	X			
Configure Management Server	X			
Configure Switch Parameters	X			
Configure Fabric Parameters	X			
Modify Port Binding	X			
Configure Open Trunking	X			

Table 3 Permissions required for feature functions (continued)

Element Manager rights	Device administration	Device operation	Device maintenance	Security administration
Configure Ports:				
Blocked	X	X	X	
LIN alerts	X	X		
Name	X	X		
Port binding	X			X
RX BB_Credit	X	X		
Speed	X	X		
Configure SNMP	X			
Configure Switch Binding:				
Connection policy				
Enable	X			X
Membership list	X			X
	X			X
Configure Threshold Alerts	X			
Configure Zoning	X			
Data Collection			X	
Date/Time Sync Configuration	X	X	X	
Enable Call Home Notification	X		X	
Enable E-Mail Notification	X		X	
Enable Telnet	X			
Enable Embedded Web Server	X			
Export Configuration Report	X	X	X	
FRU Beaconing			X	
FRU Switchover			X	

Table 3 Permissions required for feature functions (continued)

Element Manager rights	Device administration	Device operation	Device maintenance	Security administration
IPL	X	X	X	
Manage Firmware			X	
Port Diagnostics			X	
Port Beaconsing	X	X	X	
Set Online State	X	X	X	
Swap Ports (FICON management style only)	X		X	
Reset Configuration			X	
Reset Statistics Counters (Performance view)	X	X		
Reset Port	X		X	
Unit Beaconsing	X	X	X	
SANtegrity Authentication (in Element Manager and Security Center)	X			X
View Event Log		X	X	X
View Firmware			X	
View Hardware Log	X	X	X	
View LIN Log	X	X	X	
View Open Trunking Log	X		X	
View SNMP	X	X	X	
View Threshold Alert Log	X	X	X	

Backing up and restoring Element Manager data


You can protect your data by backing it up and then restoring it as necessary.

What is backed up?

The following data, contained in the <Install_Home>\Server, <Install_Home>\Client, and <Install_Home>\Call Home directories, are backed up to disk:

 **NOTE:** <Install_Home> refers to the directory where the HAFM application is installed.

- All log files.
- Zoning library (all zone sets and zone definitions). Note that zoning is configured through HAFM.
- Call-home configuration (including phone numbers and dialing options).
- Configuration data.

 **NOTE:** This data can also be saved through the **Backup & Restore Configuration** option on the Element Manager **Maintenance** menu.

- Plans. Data is saved if the optional Planning feature is available through HAFM.
- License information
- User launch scripts.
- User defined sounds.
- All data exported through the **Export** option on the HAFM **SAN** menu.

 **NOTE:** Firmware files are NOT backed up.

Backing up to a CD

The rack-mount HAFM appliance is backed up to a compact disk, rewritable (CD-RW). As long as a CD-RW disk remains in the CD recorder drive of the HAFM appliance, critical information from both the Element Manager and the HAFM are automatically backed up to the CD-RW disk when the data directory contents change or when you reboot HAFM.

Restoring data from a CD

To restore data to HAFM, copy the three folders from the CD-RW (D: \Backup\) and paste them in C:\Program Files\<Install_Home>. You will be asked if you want to overwrite the existing files; click **Yes**.

Manual backup procedures

A *full* data backup occurs the first time that you configure any parameter on a new HAFM appliance. See “[What is backed up?](#)” on page 48 for a list of data backed up for a complete backup.

After this initial backup, a backup only occurs when any data changes or if the HAFM appliance is rebooted. This backup is not a full backup, but only an incremental backup of changed data.

You should do a manual backup to ensure that HAFM data is fully backed up to a CD-ROM disk if any of the following occur:

- You are changing or archiving these disks.
- You have changed a disk and a `Use current disk` message displays.

To manually backup HAFM data:

1. Locate these folders on `C:\<Install_Home>`, where `<Install_Home>` refers to the directory where the HAFM application is installed:
 - `\Server`
 - `\Client`
 - `\Call Home`
2. Copy these folders to `X:\backup`, where `X` is the drive letter for your CD-ROM drive where backups occur. Overwrite the existing files.

2 Monitoring and managing the director

This chapter describes how to use the features available through the Element Manager to monitor and manage director operation. These features include status indicators, menu options, and dialog boxes available through the Hardware view, Port Card view, Port List view, Node List view, Performance view, and FRU List view.

- [Hardware view](#), page 51
- [Port Card view](#), page 63
- [Port List view](#), page 72
- [Node List view](#), page 75
- [Performance view](#), page 79
- [FRU List view](#), page 84
- [Port operational states](#), page 86
- [Link incident alerts](#), page 87
- [Threshold alerts](#), page 88

Hardware view

Using this graphical view of the director, you can view status symbols and simulated light emitting diode (LED) indicators, display data. You can also use mouse functions to monitor status and obtain vital product information for the director and its hardware components. To display the Hardware view, select **Hardware** from the view tabs on the Element Manager window.

Identifying FRUs

Move the mouse pointer over parts of the director graphic in the Hardware view to display labels identifying each hardware component and its slot position in the chassis relative to identical components installed in the director. Components include:

- Port cards.
 - The Director 2/64 can contain up to 16 port cards, slot positions 15 through 0 (left to right).
 - The Director 2/140 can contain up to 32 port cards in the front of the unit (slot positions 0–1) and up to three additional port cards in the rear (slot positions 33–35). Note that blank slot position 32 relates to ports 128–131, which are internal ports.

As you move the mouse pointer over each card, labels display, identifying the card's slot number and port technology. Acronyms that may display to identify port technology, such as UPM, GSML, GXXL, FPM, UPM, GLSR, GSMR, GLSL, and GXXR, also display in the **FRU** column of the FRU List view. See "[FRU List view](#)" on page 84 for details.

- Control processor (CTP) cards. Two CTP cards are installed, slot positions 1 and 0 (left to right).
- Power supply modules.
 - Director 2/64—Two modules are installed, slot positions 1 and 0 (left to right).
 - Director 2/140—Two modules are installed, slot positions 1 and 0 (left to right).

- Cooling fan modules.
 - Director 2/64—Two modules are installed, slot positions 1 and 0 (left to right).
 - Director 2/140—Three modules are installed, slot positions 2, 1, and 0 (left to right).
- Serial Crossbars (SBAR).
 - Director 2/64—Two SBARs are installed, slot positions 1 (bottom) and 0 (top).
 - Director 2/140—Two SBARs are installed, slot positions 0 (bottom) and 1 (top).

Monitoring director operation

You can monitor the operating status of the director using the Director Status table on the Hardware view and the status bar at the bottom of the window.

Director Status table

The Status table at the top of the Hardware view displays the director's operational status, operational state, name, description, and location.

- **Status**—See "[Port operational states](#)" on page 86 for the meaning of the text that displays in the director Status table and the corresponding status symbols that display on the status bar.
- **State**—Displays one of the following:
 - **Offline**—When the director is *Offline*, all ports are offline. The ports cannot accept a login from an attached device or cannot connect to other directors. You can configure this state through the Set Online State dialog box. See "[Set online state](#)" on page 142 for instructions.
 - **Online**—All unblocked ports are able to connect with devices. You can configure this state through the Set Online State dialog box. See "[Set online state](#)" on page 142 for instructions. Note that the director automatically goes online after a power-up, an initial machine load (IML), or an initial program load (IPL).
 - **Coming online**—This is a transitional state that occurs just before the director goes online. This state normally only happens briefly, unless there is a problem reaching the online state.
 - **Going offline**—This is a transitional state that occurs just before the director goes offline. This state normally only happens briefly, unless there is a problem reaching the offline state.
- **No Link Status**—If the Ethernet network connection between the HAFM appliance and the director is down, the Hardware view displays the front and rear of the unit without FRUs. The Status table at the top of the Hardware view changes to display the status (No Link) and the associated reason with a yellow background. The name, description, and location fields are blank.

The **Reason** field on the director Status table displays one of the following reasons when there are no links:

- **Never Connected**—A network connection was never established between the director and the HAFM appliance if the CTP card fails. Check the IP addresses, the Ethernet local area network (LAN) physical connection between the director and HAFM appliance, and other network connection conditions.

- **Link Timeout**—The network connection that was established between the director and HAFM appliance has been lost. Check the IP addresses, the Ethernet LAN physical connection between the director and HAFM appliance, IP addresses, and other network components.
- **Protocol Mismatch**—The director and the HAFM appliance are not at compatible software release levels. Update either HAFM or your firmware version.
- **Duplicate Session**—A link has previously been established between the director and another instance of the HAFM appliance. Connect to the previously established HAFM appliance from the HAFM login screen.
- **Unknown Network Address**—The address defined for the director in HAFM could not be found in the domain name server (DNS). Either the name was incorrect when the director was added to the application, or the name was not available from the DNS. Check the network IP address for the director definition in the application by right-clicking the product icon and choosing **Properties**. The IP address displays in the **Network Address** field.
- **Incorrect Product Type**—The product at the configured network address is not a director. Verify address, configuration, and product type.

Status bar status indicator

The status bar displays a colored status symbol that indicates the overall operating status of the director unit. The operating status depends on hardware component failures, which are indicated by status symbols that display over component graphics in the Hardware view. See ["Status bar"](#) on page 42 for the meanings of status symbols on the status bar.

The status bar indicates the director operating status based on component failures. For example, for a single port failure, a blinking red and yellow diamond displays on the port connector in the Hardware view. At the same time, a yellow triangle displays on the status bar to indicate a degraded director. However, if a blinking red and yellow diamond displays over both fan modules, the status bar displays a red and yellow diamond, indicating a failure that requires immediate attention.

Monitoring hardware operation

Determine hardware component operating status and states by the simulated LED indicators and status symbols that display on port cards, CTP cards, power supplies, fan modules, and SBAR cards illustrated in the Hardware view.

- Green and amber indicators illuminate on each FRU to indicate either an operational or degraded state, respectively. LEDs for individual ports do not illuminate on port cards in the Hardware view, but do illuminate in the Port Card view for each port. See ["Port Card view"](#) on page 63.
- Status symbols, such as flashing red and yellow diamonds and yellow triangles, display on FRUs to reflect the overall state of the hardware as changes occur.
- Corresponding or additional descriptions of hardware status and states also display when you click components to display Properties dialog boxes.

[Figure 12](#) on page 54 illustrates the Director 2/64 hardware view. [Figure 13](#) on page 55 illustrates the Director 2/140 hardware view.

NOTE: Each illustration contains examples of symbols and simulated LED indicators that can help you monitor hardware operation. Numbers by each example are keyed to descriptions that follow.

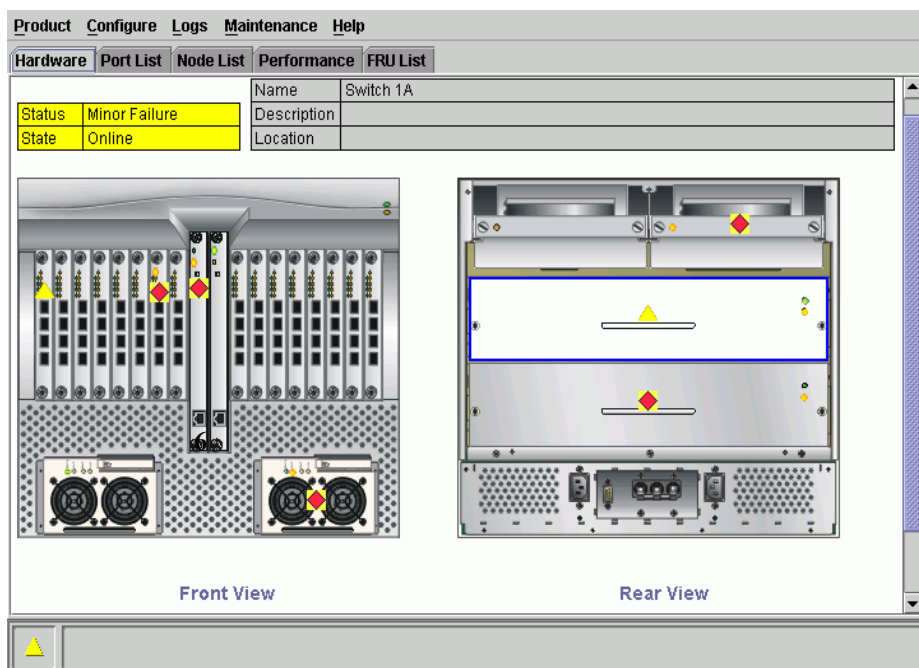


Figure 12 Monitoring hardware operation - Director 2/64 Hardware view

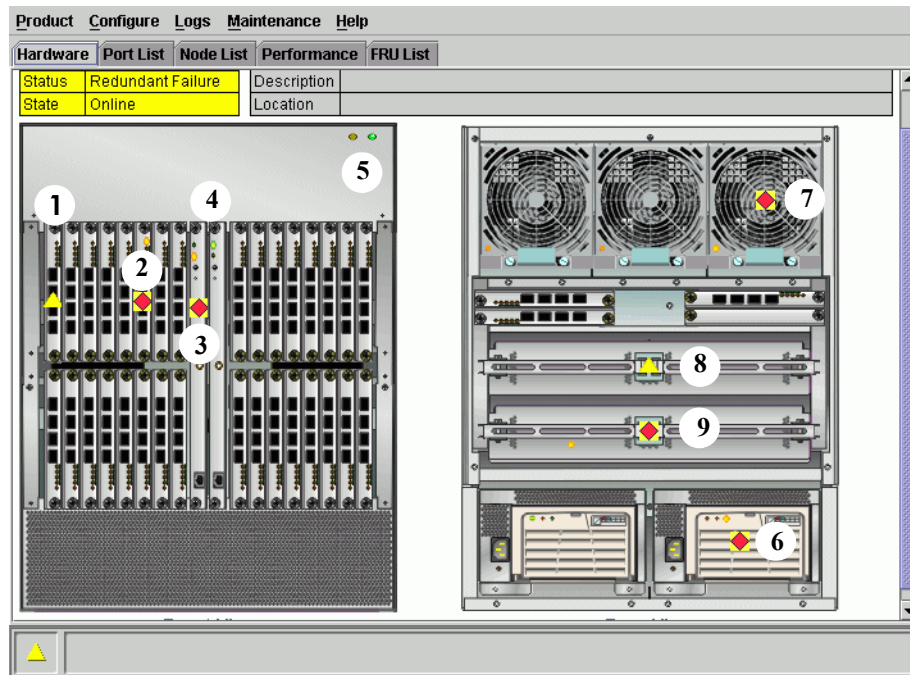


Figure 13 Monitoring hardware operation - Director 2/140 Hardware view

1. **Port card attention indicator**—The yellow triangle status symbol (▲) indicates that the port card is in a degraded state. This could indicate a problem with an individual port, such as a link failure or service-required status. A yellow triangle could also indicate that a port is in beaconing state. Open the Port Card view by double-clicking the port card to examine individual port status. See ["Port Card view"](#) on page 63 for details.
2. **Port card failure indicator**—The blinking red and yellow diamond (◆) displayed on the port card with the amber port card LED illuminated may indicate that the card has failed. This may also indicate that an individual port has failed on the card. Open the Port Card view by clicking the port card to examine individual port status. If an individual port has not failed, the card is at fault.
See ["Port Card view"](#) on page 63 for details on using the Port Card view. See ["Port operational states"](#) on page 86 for details on port operating states and the status symbol and indicator operation.
3. **CTP card failure indicator**—The blinking red and yellow diamond (◆) on the CTP card with the amber LED illuminated indicates that the card has failed.
4. **Active CTP card indicator**—The green LED on a CTP card illuminates to indicate that the card is active. Since the redundant CTP card on the left has failed, this CTP card has become the active card. If both CTP cards are operational, no LEDs illuminate on the backup card, while the green LED illuminates on the active CTP card.
5. **Power, system error, and unit beaconing indicators**—The green and amber indicators on the far right of the front bezel simulate the power and system error LEDs on the actual director bezel.

- **Power indicator**—The green indicator simulates the power LED on the actual director. When the indicator illuminates, the director is connected to facility AC power and is operational. The indicator will be on if either power supply is operating.
- **System error indicator**—The amber system error light indicator (illuminated in the Hardware views as shown in [Figure 12](#) on page 54) simulates the system error light on the actual director. When this indicator illuminates, an event has occurred requiring immediate attention, such as a system, fan, power supply, or port failure. View details of system errors by choosing **Event Log** from the **Logs** menu on the menu bar. The indicator in the Hardware view and the LED on the actual unit remains illuminated until you clear the event by right-clicking on the director graphic, away from an FRU, and choosing **Clear System Error Light** from the pop-up menu.



NOTE: If the amber LED flashes, this indicates that unit beaconing has been enabled for the director. Enable or disable unit beaconing by right-clicking on the director graphic, away from an FRU, and choosing **Enable Unit Beaconing** from the pop-up menu.

6. **Power supply failure indicator**—When a blinking red and yellow diamond (🔴🟡) displays on a power supply with the amber *Fault* indicator illuminated, the power supply has failed. The backup power supply has taken over to supply DC voltage to the director.



NOTE: A green indicator displays and no status symbols display if the power supply is working, as shown on the left (position 1) in [Figure 12](#) on page 54 and [Figure 13](#) on page 55.

7. **Cooling fan module failure indicator**—When a blinking red and yellow diamond (🔴🟡) displays on a fan module with the amber LED indicator illuminated, the module has failed or is rotating insufficiently.
8. **SBAR card beaconing indicator**—The yellow triangle status symbol (🟡) displaying on the SBAR card, with the amber LED illuminated, indicates that beaconing has been enabled.
9. **SBAR failure indicator**—The blinking red and yellow diamond (🔴🟡) displaying on the SBAR card with the amber LED illuminated indicates a card failure.

Obtaining hardware information

This section explains how to access the FRU Properties, Port Properties, and Director Properties dialog boxes.

Displaying FRU information

Double-click a CTP card, power supply, cooling fan module, or SBAR card in the Hardware view to display an FRU Properties dialog box. This dialog box displays the FRU name, slot position relative to identical FRUs installed in the chassis, active or failed state, beaconing state (CTP card and SBAR card) part number, and serial number. For the CTP card's dialog box, the Speed Capability of the card displays as either 1 Gig or 2 Gig.

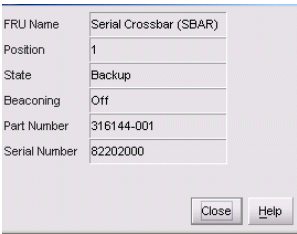


Figure 14 FRU Properties dialog box

 **NOTE:** You can display a properties dialog box for all FRUs by right-clicking on the FRU and choosing FRU Properties from the menu.

Display a Properties dialog box for a port card by right-clicking on a card and choosing **FRU Properties** from the menu. To display a properties dialog box for an individual port, you must be in the Port Card view. See "[Port Card view](#)" on page 63 for details.

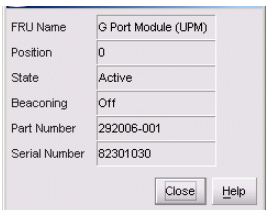


Figure 15 Port Card FRU Properties dialog box

Displaying director information

Double-click the director illustration, away from a hardware component, to

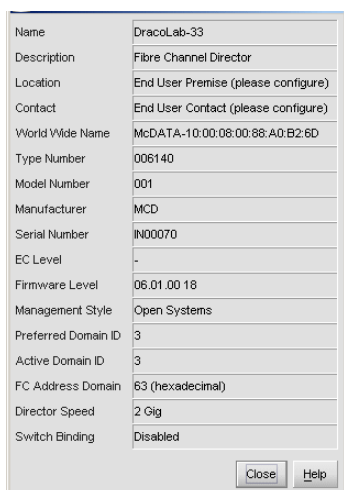


Figure 16 Director Properties dialog box

The following information displays in this dialog box:

- Director name, description, location, and contact configured through the Configure Identification dialog box.
- Fibre Channel World Wide Name (WWN) identifier for the director.
- Type Number.
- Model Number.
- Manufacturer.
- Serial Number.
- Engineering change (EC) Level.
- Firmware Level.
- Management Style—Open Systems or FICON management style.
- Preferred Domain ID—This is set through the Configure Switch Parameters dialog box.
- Active Domain ID—The actual domain ID assigned to the director.
- FC Address Domain—The director's Fibre Channel address (hexadecimal)
- Director Speed—For the Director 2/140 model, this is always 2 Gig. For the Director 2/64 model, this speed is configured through the Configure Switch Parameters dialog box and can be either 1 Gig or 2 Gig.
- Switch Binding—Displays `Enabled` if the optional SANtegrity Binding features are installed and enabled. Otherwise, displays `Disabled`.

You can also display the Director Properties dialog box by right-clicking the director illustration away from an FRU and choosing **Properties** from the menu.

Using menu options


Right-click various parts of the Hardware view to display pop-up menu options for displaying status and information and for controlling the director and its FRUs. The following menus are available:

- **Director**
- **Port Card**
- **CTP Card**
- **SBAR Card**


Director menu

Right-click any area of the director illustration where a hardware component is not installed to display the following menu options:

- **Properties**—Click this option to display the Director Properties dialog box. See details under [“Displaying director information”](#) on page 58. You can also display this dialog box by double-clicking an area on the director illustration, but not on a hardware component.
- **Enable Unit Beacons**—Click this option to toggle unit beacons on or off. When the check box has a check mark, unit beacons are on, and the amber system error light on the director front bezel blinks to help users locate the actual unit in an equipment room. When you click the check box to remove the check mark, unit beacons are disabled and the amber LED goes out.

 **NOTE:** You can only enable beacons if there are no system errors (the system error light is off).

- **Clear System Error Light**—Turns off the amber system error LED, located below the green power LED on the director front bezel.
- **IPL**—Initiates an IPL on the director. When the dialog box displays confirming the IPL, click **Yes**. For more information, see the *HP StorageWorks Director 2/64 service guide* for the Director 2/64 and the *HP StorageWorks Director 2/140 service guide* for the Director 2/140.


 **NOTE:** An IPL is not intended for ordinary or casual use and should only be performed when directed by your support personnel.

- **Date/Time**—Displays the Configure Date and Time dialog box, as shown in [Figure 17](#) on page 60.

The dialog box displays with a check mark (the default) in the **Periodic Date/Time Synchronization** check box. If this field is checked, the HAFM appliance periodically sets the director time to automatically synchronize with the HAFM appliance time. Daylight savings time automatically updates on the director using this option.

The current date and time display in the **Date** and **Time** fields. If the **Periodic Date/Time Synchronization** field is checked, the **Date** and **Time** fields are disabled (grayed out).

To enable and disable **Periodic Date/Time Synchronization**, click the check box and then click **Activate**.

 **NOTE: FICON management style only**—An error results if periodic synchronization and clock alert mode are enabled (see “[Configuring the FICON management server](#)” on page 156).

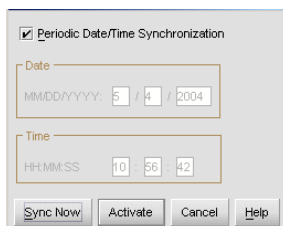


Figure 17 Configure Date and Time Periodic Synchronization dialog box

To immediately synchronize the director date and time with the HAFM appliance, be sure the **Periodic Date/Time Synchronization** option is enabled and then click **Sync Now**.

 **NOTE:** If you enable the **Periodic Date/Time Synchronization** option and click **Activate**, the time will synchronize at the next update period.

To set the director with a specific date and time, make sure that the **Periodic Date/Time Synchronization** field is not selected (see [Figure 18](#)). Enter the date and time, and then click **Activate**.

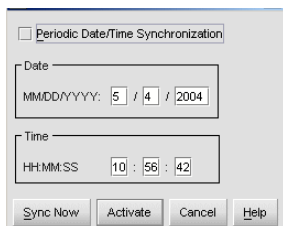


Figure 18 Configure date and time (manually)

 **NOTE:** Use the range of 0 to 23 for hours. Use the range of 0 to 59 for minutes and seconds.

- **Set Online State**—Displays the Set Online State dialog box. The dialog box displays the current state (offline or online) and provides a button for changing the state.

△ **CAUTION:** Before setting the director offline, warn administrators and users currently operating attached devices that the director is going offline and that there will be a disruption of port operation. Also, request that the devices affected by an interruption of data flow be set offline.

Click **Set Offline** or **Set Online** to toggle between offline and online states.

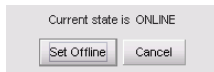


Figure 19 Set Online State dialog box (director is online)

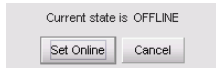


Figure 20 Set Online State dialog box (director is offline)

When the **Set Online** or **Set Offline** warning dialog box displays, click **OK** to set the director online or offline.

As the director goes offline, the word *Offline* displays in the **State** field in the left corner of the Hardware view. As the director goes online, the word *Online* displays in the **State** field in the left corner of the Hardware view. When going offline, LED indicators on all ports with attached devices stay green, but the director sends offline sequences (OLS) to these devices.

Port Card menu

Right-click a port card in the Hardware view to display the following menu options.

- **Open Port Card View**—Opens the Port Card view. You can also open the Port Card view by clicking the port card. See “[Port Card view](#)” on page 63 for detailed information.
- **FRU Properties**—Displays the port card’s Properties dialog box. This dialog box includes the FRU name, position (slot number in backplane), state (active or failed), beaconing state (on or off) part number, and serial number (see [Figure 15](#) on page 57).
- **Enable Port Card Beaconing**—Adds a check mark to the check box and enable beaconing for the card. This causes the amber LED on the card to flash to help you locate the card in the unit. Note that you cannot enable beaconing if the card has failed.
- **Block All Ports**—Displays the Block All Ports dialog box. Click **Yes** to block all ports on the selected card or **No** to cancel.
- **Unblock All Ports**—Displays the Unblock All Ports dialog box. Click **Yes** to unblock all ports on the selected card or click **No** to cancel.
- **Diagnostics**—Displays the Port Diagnostics dialog box. Use this dialog box to run internal loopback and external loopback tests on any port or all ports on the port card.


Port menu

To display the menu options for a port on a port card, open the Port Card view by double-clicking a port on the port card. See “[Port Card view](#)” on page 63” for details about displaying and using the port menu.

CTP Card menu

Right-click the CTP card in the Hardware view to display a menu with the following options:

- **FRU Properties**—Click this option to display an FRU Properties dialog box for the CTP card. The FRU Properties dialog box includes the FRU name, position (slot number in the backplane), state (active, backup, or failed), part number, and serial number.
- **Enable Card Beacons**—Click this option to add a check mark to the check box and enable beaconing for the CTP card. This causes the amber LED on the card to flash to help you locate it in the unit. Note that you cannot enable beaconing if the card has failed.
- **Switchover**—Click this option to display the Switchover CTP dialog box as shown in [Figure 21](#). Click **Switchover** to switch operations from the active card to the backup card. When switchover occurs, the green LED illuminates on the backup CTP card to indicate that it is active.

 **NOTE:** You must have maintenance authorization rights to access this feature.

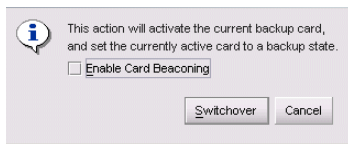


Figure 21 Switchover CTP dialog box


If you click **Enable Beacons**, the amber LED beacons (blinks) on the card that was the active card before switchover.

If a redundant card has failed, or is not installed, choosing **Switchover** displays an error message explaining that two operational cards must be installed to use this feature.

SBAR Card menu

Right-click an SBAR card in the Hardware view to display a menu with the following options:

- **FRU Properties**—Click this option to display an FRU Properties dialog box for the card. The FRU Properties dialog box includes the FRU name, position (slot number in the backplane), state (active, backup, or failed), part number, and serial number.
- **Enable Card Beacons**—Click this option to add a check mark to the check box and enable beaconing for the SBAR card. This causes the amber LED on the card to flash to help you locate it in the unit. Note that you cannot enable beaconing if the card has failed.
- **Switchover**—Click this option to display the Switchover SBAR dialog box, which is similar to the Switchover CTP dialog box shown in [Figure 21](#). Click **Switchover** to switch operation from the active card to the backup card. When switchover occurs, the green LED illuminates on the backup SBAR card to indicate that it is now the active card.

 **NOTE:** You must have maintenance authorization rights to access this feature.

If you click **Enable Beacons**, the amber LED beacons (blinks) on the card that was the active card before switchover.

Port Card view

In the Hardware view, double-click a port card or right-click a port card and select **Open Port Card View** for a detailed view of the port card, as shown in [Figure 22](#) on page 63. In this view, colored indicators reflect functions of the actual LEDs on the card. The table in the Port Card view displays the port operating state and vital product information.

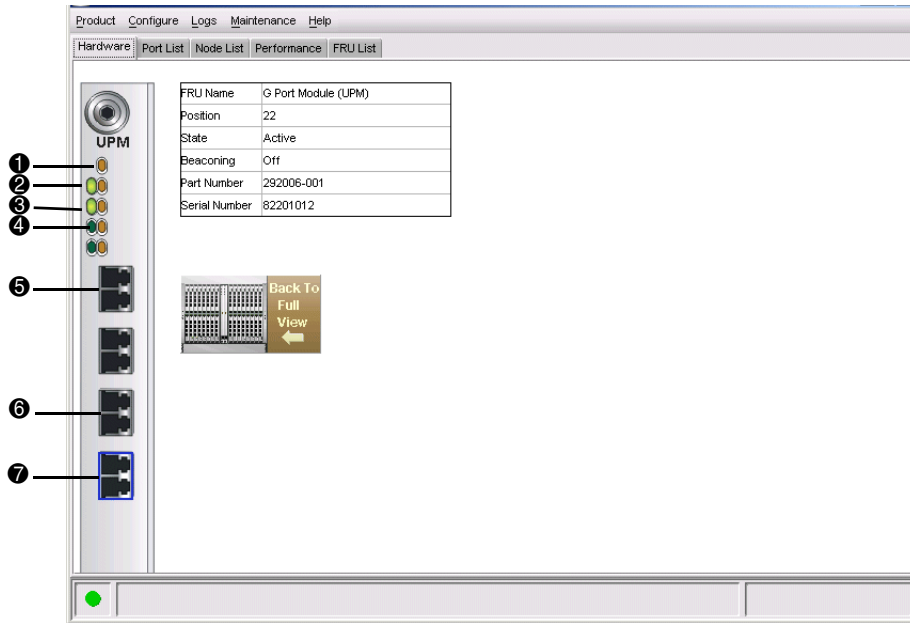


Figure 22 Port Card view

The numbered paragraphs that follow describe the numbered status symbols and LED indicators shown on the Port Card view in [Figure 22](#). Port states are described in detail under [“Port operational states”](#) on page 86.

1. The amber indicator at the top of a port card illuminates when the port card fails. A port card fails when one or more individual ports fail.
Four sets of green and amber LEDs beneath the amber card status indicator correspond to the four port connectors installed vertically down the port card.
2. In [Figure 22](#), the amber LED is blinking (while the green LED is on) for the first port on the card, and a yellow triangle displays by the port's connector. This indicates that beaconing is enabled for the port and the port is in an online state. Note that if the amber port indicator flashes and the green indicator is off, the port is running diagnostics.
The green indicator illuminates when the port is online with an attached device and fully operational. The green port LED remains on as long as the port remains in the online state. The green LED on the physical card flashes when there is active Fibre Channel traffic through the port. It does not flash in the Port Card view.

3. When the port is operational but not communicating with an attached device, the green indicator remains off. In this case, there may not be a fiber cable attached, no light from the device (the device switch is powered off), the port may be blocked, or the link may be recovering.
4. If the port fails, the amber indicator for port illuminates and a blinking red and yellow diamond displays next to the port connector.
5. A yellow triangle (attention indicator) displays next to a port connector for a variety of reasons:
 - Beacons for the port was enabled through the **Enable Beacons** option. Note that this is the case in the illustration on [Figure 22](#) on page 63 (see number 1 in the illustration).
 - The port is receiving the Not Operational sequence from the attached device.
 - The port has an invalid attachment.
 - The director and attached device are performing a link reset operation.
 - LIN status symbols have been enabled for a port in the Configure Ports dialog box and a link incident occurs.
 - A threshold status has occurred for the port.
 - Diagnostics are running on the port.
6. The Port Card view indicates a failed port by a blinking red and yellow diamond status symbol by the port's connector. The amber LED for the port will also be illuminated (see number 4 in [Figure 22](#) on page 63).
7. A blank port indicates that the port optics are not installed.

Displaying port information

Double-click a port or right-click a port and select **Port Properties** from the menu to display the port's Properties dialog box, as shown in [Figure 23](#). You can also display this dialog box by:

- Double-clicking on a row in the Port List view or right-clicking on a row and choosing **Port Properties** from the menu.
- Double-clicking on a port's bar graph in the Performance view or right-clicking on the bar graph and choosing **Port Properties** from the menu.
- Right-clicking on a port's row in the Node List view and choosing **Port Properties** from the menu.
- Right-clicking on a port's row in the Port List view and choosing **Port Properties** from the menu.

- Clicking a port, port row, or port bar graph in the preceding views and choosing **Port Properties** from the secondary **Port** menu in the **Product** menu on the menu bar.

Port Number	10
Port Name	
Type	F_Port
Operating Speed	1 Gb/s
Port WWN	McDATA-100E08086A02104
Block Configuration	Unblocked
RX BB Credits Configured	0
Logged in IDs	1
LIN Alerts Configuration	On
FAN Configuration	Off
Beaconing	Off
Link Incident	None
Operational State	Online
Reason	
Threshold Alert	
Zoning Enforcement	Hard Zoning

Figure 23 Port Properties dialog box

The following paragraphs describe the fields in the Port Properties dialog box.

- Port Number**—The physical port number.
- Port Name**—User-defined port name or description. See ["Configuring ports"](#) on page 97 for instructions.
- Type—The type of port.**
 - G_Port**—This displays if nothing is logged into the port.
 - F_Port**—This displays if a device is logged into the port.
 - E_Port**—This displays if the port is connected to another director's E_Port via an ISL.

If a port is configured to be a specific port type, that configured type displays regardless of whether the port is connected to anything or not.

- Operating Speed**—This field displays the current data speed for the port as 1 Gig, 2 Gig, or Not Established. Not Established displays if **Negotiate** was set for the port through the Configure Ports dialog box and the data speed has not been resolved between the port and the attached device, or if the port and device are not communicating.
- Fibre Channel Address**—The port's Fibre Channel address identifier.
- Port WWN**—The port's 16-digit World Wide Name (WWN).
- Attached Port WWN**—The WWN of the node logged into the port.
- Block Configuration**—Blocked or Unblocked. Operation can be blocked or unblocked by one of the following methods:

- Through the Configure Ports dialog box.
- Through the **Block All Ports** or **Block Port** option on right-click menus in the Port Card view.
- Right-clicking on the port in the Hardware view, the Port List view, or the Performance view and choosing **Block Port** from the menu.
- Through the **Product Port** menu in the Hardware view, the Port List view, or the Performance view.

See “[Configuring ports](#)” on page 97 and “[Port Card view](#)” on page 63 for details.

- **10-100 km Configuration**—Extended distance buffering. This can be enabled or disabled for the port through the Configure Ports dialog box. See “[Configuring ports](#)” on page 97 for instructions.
- **LIN Alerts Configuration**—This field indicates whether LIN alerts are enabled or disabled. LIN alerts can be configured through the Configure Ports dialog box. The default is for the LIN alerts to be enabled.
- **Beaconing**—This field indicates the beaconing status for the port. To enable or disable beaconing, right-click the port and select **Enable Beaconing**.
- **Link Incident**—Description of the last link incident that occurred on the port.
- **Operational State**—Beaconing, inactive, invalid attachment, link incident, link reset, no light, not operational, online, offline, port failure, segmented E_Port, testing. See “[Port operational states](#)” on page 86 for definitions of operational states.
- **Reason**—Lists the reason for a segmented E_Port, invalid attachment, or inactive operating state for the port. When an E_Port is segmented, two fabrics are prevented from joining. An E_Port segmentation only occurs when the director is connected to another director or a switch. This field displays “NA” if a segmented E_Port or invalid attachment operating state has not occurred.

Refer to the section on joining zoned fabrics in the *HP StorageWorks SAN High Availability Planning Manual*.

The following messages display in the **Reason** field of the Port Properties dialog box if an Invalid Attachment, Segmented E_Port, or Inactive state occurs for the port. Reason messages for segmentation can include:

- **Incompatible operating parameters**—Operating parameters, such as resource allocation time-out values (R_A_TOV) or error-detect time-out values (E_D_TOV), are inconsistent on connected switches. See “[Configuring fabric parameters](#)” on page 95 for more information.
- **Duplicate domain IDs**—Identical preferred domain IDs are configured for two or more directors or switches. See “[Configuring fabric parameters](#)” on page 95 for more information.
- **Incompatible zoning configurations**—Refer to the *HP StorageWorks HA-Fabric SAN High Availability Planning Guide* for information on joining zoned fabrics.
- **Build fabric protocol error**.
- **No principal switch**—A principle switch is not defined for the fabric.
- **No response from the attached switch**.

A Port Binding error may be due to an invalid WWN or nickname entry in the Configure Ports dialog box in the **Bound WWN** column. See "[Configuring ports](#)" on page 97 for a description of the Configure Ports dialog box.


Reason messages for an invalid attachment can include:

- 0x0C ESA Security Mismatch—Security features do not match.
- 0x0D Fabric Binding Mismatch—Fabric Binding is enabled and detected a connection with a switch or director with an incompatible fabric membership list.
- 0x0E Authorization Failure Reject—The switch or director on the other side of an ISL detected a security violation. Your switch received notification via a generic reject code and sets its port to the invalid attachment state in sympathy.
- 0x0F Unauthorized Switch Binding WWN—A Switch Binding error was detected on either an E_Port or an F_Port.
- 0x10 Authentication Failure—ISL Authentication Check (CHAP) failed.
- 0x11 Fabric Mode Mismatch—A connection was not allowed because:
 - An HP M-Series switch or director attempted to connect to an HP switch or director running in Open Fabric mode.
 - An HP M-Series switch or director running in Open Fabric mode attempted to connect to another vendor's switch or director with an incorrect exchange link protocol (ELP) revision level.
- 0x12 CNT WAN Extension Mode Mismatch—The ELP maximum frame sizes were incompatible because one product running in CNT WAN extension mode attempted to connect to another product running in a normal mode.
- 01 Unknown—The reason is not known.
- 02 ISL connection not allowed on this port—ISL is connected to a port configured as an F_Port.
- 03 ELP rejected by the attached switch—This director transmitted an exchange link protocol (ELP) frame that was rejected by the switch at the other end of the ISL.
- 04 Incompatible switch at other end of the ISL—The switch is configured for Homogenous Fabric mode, and the switch at the other end of the ISL is an HP switch configured for Open Fabric 1.0 mode.
- 05 External loopback adapter connected to the port—A loopback plug is connected to the port, and no diagnostic test is running.
- 06 N_Port connection not allowed on this port—The port type configuration does not match the actual port use (the port is configured as an E_Port, but attaches to a node device).
- 07 Non_HP switch at other end of the ISL—The cable is connected to a non-HP switch, and interop mode is set to Fabric 1.0 mode.
- 08 ISL connection not allowed on this port—The port type configuration does not match the actual port use (the port is configured as an F_Port, but attaches to a director or switch).

- 10 Port binding violation - Unauthorized WWN—The WWN that was entered to configure Port Binding for this port is not valid, or a nickname was used that was not configured for the attached device in the Element Manager.
- 11 Unresponsive node connected to port—Possible causes are: (1) a hardware problem on a switch or connected node where ELP frames are not delivered; the response is not received, or a fabric login (FLOGI) cannot be received (there may be problem in the switch SBAR); (2) a faulty or dirty cable connection; (3) faulty host bus adapters that do not send out a FLOGI within a reasonable timeframe.

Reason messages for an inactive state include:

- 1 Switch speed conflict (Director 2/64 model only)—The director data speed was set to 2 Gb/s, but the port only supports 1 Gb/s operation because it is on an FPM port card. (All ports on all installed FPM cards will go inactive if the director data speed is set to 2 Gb/s.) To activate the port, either set the director data speed to 1 Gb/s (**1 Gig**) through the Configure Switch Parameters dialog box, or replace the FPM card with a UPM card.
- 2 Optics speed conflict (Director 2/64 model only)—The port data speed was set to 2 Gb/s, but the director data speed was set to 1 Gb/s. To activate the port, set the director data speed to 2 Gb/s (**2 Gig**) through the Configure Switch Parameters dialog box. Note that a port could also be inactive if the card is an FPM card and the port data speed was set to 2 Gb/s. To activate the port in this case, set director data speed to 1 Gb/s, or replace the FPM card with a UPM card.

 **NOTE:** Note that your director model and firmware may not allow variable data speed settings.

- **Threshold Alert**—If a threshold alert exists for the port, an alert indicator (yellow triangle) displays by the **Threshold Alert** field, and the configured name for the last alert received displays in the field.
- **Zoning Enforcement**—For directors, this field displays **Soft zoning** for ports using soft zoning and **Hard zoning** for ports using hard zoning.


Port Card menu

While in the Port Card view, right-click the card away from a port connector to display a pop-up menu of port card functions.

- **Block All Ports**—Click this option to display the Block All Ports dialog box. Click **Yes** to block all ports on the selected card or click **No** to cancel.
- **Unblock All Ports**—Click this option to display the **Unblock All Ports** dialog box. Click **Yes** to unblock all ports on the selected card or **No** to cancel.
- **Diagnostics**—Click this option to display the Port Diagnostics dialog box. Use this dialog box to run internal loopback and external loopback tests on any port or all ports on the port card. For instructions on using these diagnostics, refer to the *HP StorageWorks Director 2/64 service guide* for the Director 2/64 and the *HP StorageWorks Director 2/140 service guide* for the Director 2/140.

Port menu

While in the Port Card view, right-click any port to display the following menu options:

- **Port Properties**—Click this option to display the Port Properties dialog box. This dialog box displays information about the port. See [“Displaying port information”](#) on page 64 for more information.
- **Node Properties**—Click this option to display the Node Properties dialog box. Note that if a node is not logged into the port, a message displays indicating that node information is not available. For details on information that displays in this dialog box, see [“Displaying node properties”](#) on page 77.
- **Port Technology**—Click this option on the **Port** menu to display the Port Technology dialog box. You can also display this dialog box by choosing **Port Technology** from the right-click menu in the Port List view. This dialog box displays the following information:
 - **Port number**
 - **Connector type**—Always LC.
 - **Transceiver type**—Longwave laser LC or shortwave laser LC.
 - **Distance**—General distance range for port transmission. This can be either short to long distances for the longwave laser LC transceiver or short distances for the shortwave laser LC transceivers.
 - **Media**—The Fibre Channel mode and optic size. For the longwave laser LC transceiver, this would be singlemode 9 micron. For the shortwave laser LC transceiver, this would be multimode 50-micron or 62.5-micron.
 - **Speed**—This will be either 1 Gb/s or 2 Gb/s.
- **Block Port**—Click this option to display a check mark and block port transmission. If blocked, a node attached to the port is prevented from logging into the director or communicating with other devices attached to director ports. A blocked port continuously transmits offline signals (OLS). Click to remove the check mark and unblock the port. If unblocked, a node attached to the port can communicate with the director and communicate with other nodes attached to the director.
- **Enable Beaconing**—Click this option to make the amber LED by the port blink on the actual director and the amber indicator blink for the port in the Hardware view. This enables users to locate the unit where the port is located. When a blinking amber LED indicator displays by a port, an attention indicator () displays below the port's connector in the Port Card view, Port List view, and on the Port card in the Hardware view. Note that beaconing cannot be enabled for a failed port.
- **Port(s) Diagnostics**—Click this option to display the Port Diagnostics dialog box. Use this dialog box to run an internal loopback and external loopback test on the port. The **Port(s) Diagnostics** option enables you to run internal and external loopback tests on any port or all ports on a port card. To use this option, follow the detailed steps in the *HP StorageWorks Director 2/64 service guide* for the Director 2/64 and the *HP StorageWorks Director 2/140 service guide* for the Director 2/140.

- **Channel Wrap** (FICON management style)—Click this option while in FICON management style to display a check mark and allow a channel wrap test to be initiated from an attached host or device. In this test, frames are sent to the director port, then the director echoes the frames back to the sending device to test the channel. The director remains in channel wrap mode until the option is disabled. While in channel wrap mode, the port can only accept echo commands from the host and displays to be blocked to all other communication. Click the check box to remove the check mark and disable channel wrap.
- **Swap Ports** (FICON management style only)—Click this option while in FICON management style to display the Swap Ports dialog box. Use this dialog box to swap addresses between ports. For details, see “[Swap ports \(FICON management style\)](#)” on page 140.
- **Clear Link Incident Alert(s)**—Click this option on the port’s right-click menu on the Port Card view and the Port List view to display the Clear Link Incident Alert(s) dialog box. Click **This port only** to clear the attention indicator for the selected port on the Hardware view, the Port List view, and the Performance view. Click **All ports on director** to clear all ports. In addition, the procedure clears the alert description in port Properties dialog boxes. If there are no link incident alerts set for a port, no actions occur. Although you can manually clear link incidents, they may also be cleared by actions outside of the user interface, such as when rebooting the HAFM appliance.
- **Reset Port**—Click this option to display a confirmation dialog box. Click **Yes** to reset the port. If a switch is attached to the port and online, this operation sends a link reset to the attached switch; otherwise, this action disables port beaconing for the port. If the port is in a failed state, such as after failing a loopback test, the reset restores the port to an operational state, clearing the service required (amber) LED. The reset does not affect other ports in the director.
- **Port Binding**—Right-click any port in the Port Card view right-click menu and select **Port Binding** to display the Port Binding dialog box, as shown in [Figure 24](#) on page 70. Use this dialog box to allow a device with a specific WWN or nickname to have exclusive communication privileges over a port. To use this dialog box, see the following paragraphs.

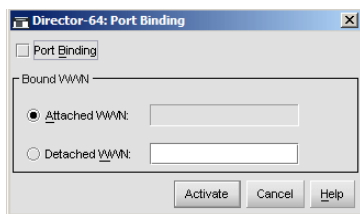


Figure 24 Port Binding dialog box

Use the Port Binding dialog box to set the following options:

- **Port Binding**—Click to place a check mark in the box and enable Port Binding for the port. When enabled, only a specific device can communicate through the port. This device is specified by the WWN or nickname entered into the **Bound WWN** field (either the **Attached WWN** or **Detached WWN** options). With the check box cleared, any device can communicate through the port even if a WWN or nickname is specified in the **Bound WWN** field.

- **Attached WWN**—Click the option button for this option and, if a device is logged into the port, the device's WWN displays in the field. The device with this WWN or nickname will have exclusive communication privileges to the port if **Port Binding** is enabled.

If you click this option button to bind the port to a logged-in device and there are no devices logged in, the port is essentially bound to a WWN of "0." This prevents any device from logging in until this button is re-enabled to bind the WWN of a logged-in device or until you explicitly bind the WWN of a device by clicking the WWN option button and entering a WWN or nickname (see the following). Changes only take effect when you click **Activate**.

- **Detached WWN**—Click the option button and enter a World Wide Name (WWN) in the proper format (xx.xx.xx.xx.xx.xx.xx.xx) or a nickname configured through HAFM. The device with this WWN or nickname will have exclusive communication privileges through the port if **Port Binding** is enabled. Note the following:
 - If you do not enter valid WWN or nickname in this field, but the **Port Binding** check box is checked (enabled), then no devices can communicate over the port.
 - If you enter a WWN or nickname in this field and do not place a check in the **Port Binding** check box, the WWN or nickname will be stored, and all devices can communicate over the port.
- **Activate**—Click to activate settings in this dialog box.

If one or more of the nodes logged into a port does not match the WWN or nickname configured in the field by the **WWN** option button, a warning dialog box displays after you activate the configuration. This warning box displays a list of all nodes that will be logged off if you continue. If you **Continue**, these nodes will be logged off and the port will only attach to the device with the device with the WWN or nickname configured in the WWN field.

An error message displays after you activate the configuration if the format for the WWN entered in the **WWN** field is not valid (not in xx.xx.xx.xx.xx.xx.xx.xx format) or if you have entered a nickname that was not configured through the Element Manager.

- **Clear Threshold Alert(s)**—Click the **Clear Link Threshold Alert(s)** option on the port's right-click menu on the Port Card view and the Port List view to display the Clear Threshold Alert(s) dialog box as shown in [Figure 25](#). Click the appropriate option to clear alerts for the selected port only or all ports on the director. This clears all attention indicators that notify users of threshold alerts in dialog boxes and views. This action also restarts the notification interval and the cumulative minutes for utilization% interval.

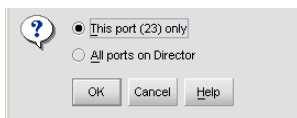


Figure 25 Clear Threshold Alert(s) dialog box

Port List view

Display the Port List view as shown in Figure 26 in the View panel by selecting the **Port List** option from the view tabs.

Product Configure Logs Maintenance Help						
Hardware Port List Node List Performance FRU List						
Port #	Name	Block Config	State	Type	Operating Speed	Alert
0		Unblocked	Offline	G_Port	1 Gig	▲
1		Unblocked	Online	F_Port	1 Gig	
2		Unblocked	Online	F_Port	1 Gig	
3		Unblocked	Online	F_Port	1 Gig	
4		Unblocked	Offline	G_Port	1 Gig	▲
5		Unblocked	Online	F_Port	1 Gig	
6		Unblocked	Online	F_Port	1 Gig	
7		Unblocked	Online	F_Port	1 Gig	
8		Unblocked	Offline	G_Port	1 Gig	▲
9		Unblocked	Online	F_Port	1 Gig	
10		Unblocked	Online	F_Port	1 Gig	
11		Unblocked	Online	F_Port	1 Gig	
12		Unblocked	Offline	G_Port	1 Gig	▲
13		Unblocked	Online	F_Port	1 Gig	
14		Unblocked	Online	F_Port	1 Gig	
15		Unblocked	Online	F_Port	1 Gig	
16		Unblocked	Offline	G_Port	1 Gig	▲
17		Unblocked	Online	F_Port	1 Gig	
18		Unblocked	Online	F_Port	1 Gig	
19		Unblocked	Online	F_Port	1 Gig	
20		Unblocked	Offline	G_Port	1 Gig	▲
21		Unblocked	Online	F_Port	1 Gig	
22		Unblocked	Online	F_Port	1 Gig	
23		Unblocked	Online	F_Port	1 Gig	

Figure 26 Port List view

The Port List view displays the following information on all ports that can be installed in the director. All information is updated automatically.

- **#**—The physical port number, from 0–63 on the Director 2/64 and 0–127 and 132–143 on the Director 2/140. Note that for this director, ports 128–131 are internal ports and not available for external connections.
- **Addr** (FICON management style only)—Displays the logical address of the port, which is the port number in hexadecimal format. For example, the address for port 0 is 4 (0+4). If port addresses have been swapped, those addresses will be followed by an asterisk (*).
- **Name**—Displays the port name as configured through the Configure Ports dialog box.
- **Block Config**—Indicates the blocked or unblocked configuration of the port as set through the Configure Ports dialog box.

The **Block Port** option is available through port right-click menus in the Hardware view, port row right-click menus in the Port List view, port bar graph right-click menus in the Performance view, and the **Port** secondary menu of the **Product** menu on the menu bar.

The **Block Port** option is also available on the port row right-click menus in the Port List view, the port bar graph right-click menus in the Performance view, and the **Port** secondary menu of the **Product** menu on the menu bar. Blocked states are:


- **Blocked**—Devices communicating with the port are prevented from logging into the director or communicating with other devices attached to director ports. A blocked port continuously transmits OLS.
- **Unblocked**—Devices communicating with the port can log into the director and communicate with devices attached to any other unblocked port in the same zone.
- **State**—The following port operational states may display in this table. For more information on these states and corresponding status symbol and LED indicator operations in the Hardware view, see ["Port operational states"](#) on page 86.
 - No Light
 - Online
 - Offline
 - Beaconsing
 - Link Reset
 - Not Operational
 - Invalid Attachment
 - Port Failure
 - Segmented E_Port
 - Link Incident
 - Testing
 - Inactive
- **Type**—The type of port.
 - It is an F_Port if an N_Port is attached.
 - It is an E_Port if another E_Port is attached.
 - It is a G_Port if the port is capable of acting as either an F_Port or an E_Port, but nothing is currently attached.
- **Operating Speed**—Displays the port speed, which may be:
 - 1 Gig if port is configured to 1 Gig
 - 2 Gig if port is configured to 2 Gig
 - Not Established if port is configured to Negotiate and no device is connected to the port
- **Alert**—Displays a yellow triangle if any alert occurs or if the port's LED is beaconsing. Blinking red and yellow diamonds display for port failures or for ports requiring service. Click the row to display the reason for the alert in the Port Properties dialog box.

Double-click a row to display the Port Properties dialog box. For an explanation of the fields on the Port Properties dialog box, see ["Displaying port information"](#) on page 64.

Port List view menu options

Right-click a row to display a menu with the following port-related action options. These are the same menu options that display when you right-click a port in the Port Card view and a port's bar graph in the Performance view. You can also click a port or bar graph in the preceding views and then click **Product > Port** on the menu bar. See "[Port menu](#)" on page 69 for an explanation of these menu options.

- **Port Properties**
- **Node Properties**
- **Port Technology**
- **Block Port**
- **Enable Beacons**
- **Port(s) Diagnostics**
- **Channel Wrap** (FICON management style only)
- **Swap Ports** (FICON management style only)
- **Clear Link Incident Alert(s)**
- **Reset Port**
- **Port Binding**
- **Clear Threshold Alert(s)**

 **NOTE:** For Node Properties, if a node is not logged in, a message displays indicating that node information is not available.

Node List view

Display the Node List view in the View panel by choosing **Node List** from the view tabs. This view displays information about all node attachments to any F_Ports on the director sorted by port number. All data is dynamic and updates automatically as devices log in and log out.


Port #	Address	Port WWN	Unit Type	BB_Credit
90	635E13	Digital Equipment -50:00:1F:E1:00:14:2C:C4	Reserved	2
94	636213	Digital Equipment -50:00:1F:E1:00:14:2C:C1	Reserved	2

Figure 27 Node List view

Information that displays for each node includes:

- **Port #**—The physical port number, from 0–63 on the Director 2/64 and 0–127 and 132–143 on the Director 2/140. Note that on the Director 2/140, ports 128–131 are internal ports and are not available for external connections.
- **Address**
 - In FICON management style, this displays the logical port address (hexadecimal of port number).
 - In Open Systems style, this displays the nodes Fibre Channel address.
- **Port WWN**—The port WWN of the attached node (N_Port). The 16-digit WWN is a set of unique numbers assigned to the device attached to the port. The WWN is prefixed by the manufacturer’s name of the host bus adapter that attaches to the device. If there is a nickname assigned, the nickname displays instead of the WWN.
- **Unit Type**—The following information, if supported, is supplied by the attached device:
 - Channel path ##, where ## will be replaced with the Channel Path Identifier (2 hex digits)
 - Communications controller
 - Converter
 - Direct access storage

- Gateway
- HBA
- Host
- Hub
- Integrated CTC adapter
- Magnetic tape
- Module
- Other
- Printer
- Proxy-agent
- Software driver
- Stand-alone CTC adapter
- Storage subsystem
- Storage device
- Switch
- Terminal (full screen)
- Terminal (line mode)
- Unit record (input)
- Unit record (output)
- Unknown
- Unspecified

 **NOTE:** The unit type comes directly from the device's sense ID when the device attaches to the port during login. If the connection is lost to the device, the type will display as `unspecified` since the device is no longer logged into the port. When the device logs back in, the unit type will update.

- **BB_Credit**—The buffer-to-buffer credit that the attached node has available.


Double-click a row to display the Node Properties dialog box. For an explanation of the fields on the Node Properties dialog box, see [“Displaying node properties”](#) on page 77.

Node List view menu options

Right-click a row to select it and display a menu with the following port-related action options:

- **Node Properties**—Displays the Node Properties dialog box. See [“Displaying node properties”](#) on page 77.
- **Port Properties**—Displays the Port Properties dialog box as shown in [Figure 23](#) on page 65.
- **Define Nickname** —Displays the Define Nickname dialog box. This dialog box allows you to define a nickname to display for the attached device instead of the device's eight-byte WWN.

To define a nickname, enter a name of up to 32 characters in the **Nickname** field and click **OK**. The nickname displays under the **Port WWN** column instead of the device's WWN.

 **NOTE:** A maximum of 2,048 nicknames are allowed.

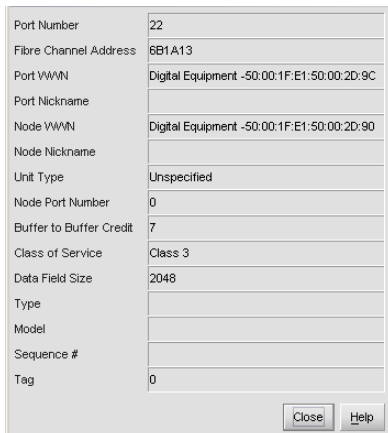
- **Display Options**—Select **Nickname** or **World Wide Name** from the submenu. Choosing **Nickname** displays attached devices in the **Port WWN** column by the nickname configured through the **Define Nickname** menu option. Selecting **World Wide Name** displays attached devices in the **Port WWN** column by the device's WWN.

Displaying node properties

You display Node properties through the Node Properties dialog box. You can use any of the following methods to open the Node Properties dialog box:

- Double-click a row in the Node List view or right-click a row and select **Node Properties** from the menu.
- Right-click a port in the Port Card view.
- Right-click a port's row in the Port List view.
- Right-click a port's bar graph in the Performance view and select **Node Properties** from the menu that displays.
- Click a port, port row, or bar graph in the views listed above and then select **Product > Port > Node Properties**.

 **NOTE:** If a node is not logged in, a message displays indicating that node information is not available.




Port Number	22
Fibre Channel Address	6B1A13
Port WWN	Digital Equipment -50:00:1F:E1:50:00:2D:9C
Port Nickname	
Node WWN	Digital Equipment -50:00:1F:E1:50:00:2D:90
Node Nickname	
Unit Type	Unspecified
Node Port Number	0
Buffer to Buffer Credit	7
Class of Service	Class 3
Data Field Size	2048
Type	
Model	
Sequence #	
Tag	0

Close Help

Figure 28 Node Properties dialog box

- **Port Number**—The physical port number on the director to which the node is connected.

- **Fibre Channel Address**—In Open Systems style only, this displays the three-byte Fibre Channel Address of the node.
- **Port Address**—In FICON management style only, this displays the logical address (hexadecimal number) for the port where the node is attached.
- **Port WWN**—Port World Wide Name of the attached device.
- **Port Nickname**—Nickname for the port WWN. Must be configured to display.
- **Node WWN**—Node World Wide Name of the attached device. Must be configured to display.
- **Node Nickname**—Nickname for the node WWN.
- **Unit Type**—See the “Unit Type” bullet on page 75 for a description.
- **Buffer-to-Buffer Credit**—The buffer-to-buffer credit that the attached node has available.
- **Class of Service**—Class of service. This can be Class 2, Class 3, or both.
- **Data Field Size**—Data field size. This is the largest size of Fibre Channel frame the node will process. The size is negotiated with the attached device.

 **NOTE:** Node Properties is also available from the menu that displays when you right-click a port's row in the Port List view or on a port's bar graph in the Performance view.

- **Type**—Type number.
- **Model**—Model number.
- **Sequence #**—Sequence number.
- **Tag**—tag number.

Performance view

Display the Performance view in the main panel by selecting **Performance** from the view tabs. This view displays a bar graph at the top of the view for all ports. The lower portion of the view displays statistical values for the specific port's bar graph that you select.

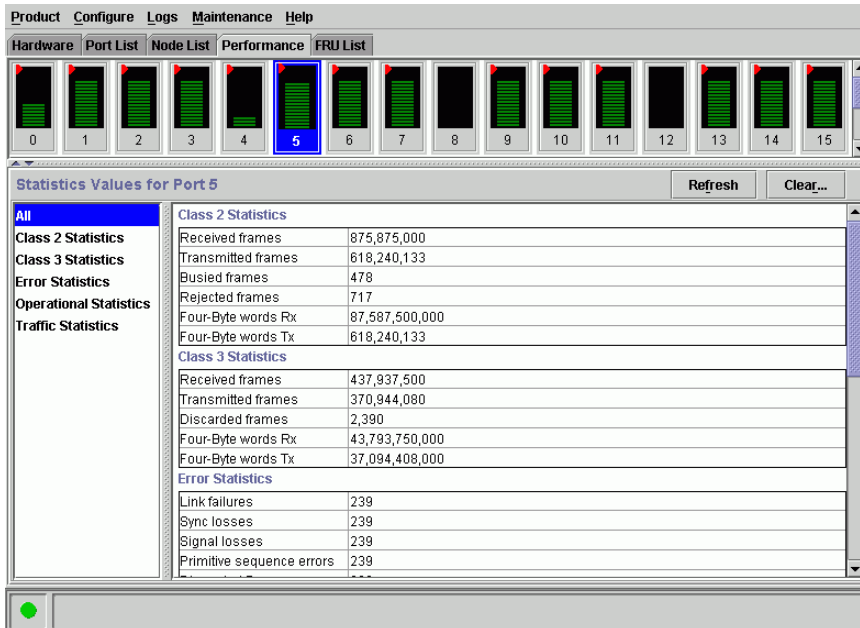



Figure 29 Performance view

Performance view menu options

Right-click any of the port bar graphs to display a pop-up menu with the following port-related action options. These are the same menu options that display when you right-click a row in the Port List view or a port in the Port Card view. You can also display these options by clicking a port, port row, or bar graph in the preceding views and choosing the secondary **Port** menu from the **Product** menu on the menu bar. See "Port menu" on page 69 for an explanation of these menu options.

- **Port Properties**
- **Node Properties**
- **Port Technology**
- **Block Port**
- **Enable Beaconsing**
- **Port(s) Diagnostics**
- **Channel Wrap** (FICON management style only)
- **Swap Ports** (FICON management style only)
- **Clear Link Incident Alert(s)**
- **Reset Port**

- **Port Binding**
- **Clear Threshold Alert(s)**

 **NOTE:** For Node Properties, if a node is not logged in a message displays indicating that node information is not available.

Bar graph display

The Performance view provides a graphical display of performance for all ports. Each bar graph in the upper portion of the View panel displays the percentage of link utilization for the port. This information updates every five seconds. A red arrow marks the highest utilization since the opening of the Performance view. If the system detects activity on a port, it represents minimal activity with one bar.

When a port is logged in, moving the mouse pointer over its bar graph displays a message with the attached port's WWN. If the port is an E_Port, the message reads "E_Port." If the port is not logged in, the message displays the port's current operational state. See "[Port operational states](#)" on page 86.


Port statistics

To select and display more detailed performance information for a port, click the port's bar graph. The bar graph for that port highlights with a darker background, and the lower portion of the Performance view panel displays the statistics values for the port's number and the WWN decoding.

The **Statistics Values** tables include values for the following categories:

- **Class 2 Statistics**
- **Class 3 Statistics**
- **Error Statistics**
- **Operational Statistics**
- **Traffic Statistics**

Click a category in the left frame of the statistics area to display only statistics for that category or click **All** to display values for all categories.

 **NOTE:** There are not thresholds for these values. You may determine that a problem exists by the rate that the value changes. For example, low BB_Credit can occur if data is sent to a device faster than it can consume the frames. This can backup into ISLs causing degraded performance.

The **Statistics Values** tables contain statistics in the following groups. To refresh tables with the latest data, click **Refresh** on the upper right portion of the **Statistics Values** panel or click the port's bar graph. Clear all counters for all users using **Clear**.

Class 2 statistics

The Class 2 statistics include:

- **Received Frames**—The number of Class 2 frames received by this F_Port from its attached N_Port.
- **Transmitted Frames**—The number of Class 2 frames transmitted by this F_Port to its attached N_Port.
- **Busied Frames**—The number of F_BSY frames generated by this F_Port against Class 2 frames. This can occur if frames are received before the switch completes initialization or if the switch is servicing so many requests that it can not process a new request. The port generates frames if the switch is not ready to accept commands. This may indicate temporary congestion.
- **Rejected Frames**—The number of F_RJT frames generated by this F_Port against Class 2 frames. These frames usually occur because of attached device errors. The device is expected to correct the error based on the reject code, then retry its request. If the device is able to recover, there is no cause for concern. If not, further troubleshooting may be necessary. There are no thresholds for this value. Typically, this occurs because the destination is not available due to the device's action.
- **Four-Byte Words Rx**—The number of four-byte words received.
- **Four-Byte Words Tx**—The number of four-byte words transmitted.

Class 3 statistics

The Class 3 statistics include:

- **Received Frames**—The number of Class 3 frames received by this F_Port from its attached N_Port.
- **Transmitted Frames**—The number of Class 3 frames transmitted by this F_Port to the attached N_Port.
- **Discarded Frames**—The number of Class 3 frames discarded, including multicast frames with bad destination identifiers (D_IDs).
The director increments this count when it discards a frame that cannot be routed. This occurs most frequently when a destination becomes unavailable without the source realizing the destination is unavailable. There are no thresholds for this value. Typically, this occurs when the destination is not available due to the destination device's action.
- **Four-Byte Words Rx**—The number of four-byte words received.
- **Four-Byte Words Tx**—The number of four-byte words transmitted.

Error statistics

Port errors indicate that a port is not operating correctly. Use this data to isolate problems with port and link operations. Error statistics include:

- **Link failures**—A link failure was recorded in response to a not operational sequence (NOS), protocol timeout, or port failure. At the Port Card view, a yellow triangle displays to indicate a link incident, or a blinking red and yellow diamond displays to indicate a port failure.

- **Sync losses**—A loss of synchronization was detected because the attached device was reset or disconnected from the port. At the Port Card view, a yellow triangle displays to indicate a link incident.
- **Signal losses**—A loss of signal was detected because the attached device was reset or disconnected from the port. At the Port Card view, a yellow triangle displays to indicate a link incident.
- **Primitive sequence errors**—An incorrect primitive sequence was received from the attached device, indicating a Fibre Channel link-level protocol violation. At the Port Card view, a yellow triangle displays to indicate a link incident.
- **Discarded frames**—A received frame could not be routed and was discarded because the frame timed out (insufficient buffer-to-buffer credit) or the destination device was not logged into the director.
- **Invalid transmission words**—The number of times that the director detected invalid transmission words from the attached device. This indicates that a frame or primitive sequence arrived at the director's port corrupted. This corruption can be due to the attached device performing a reset, plugging or unplugging the link, bad optics at either end of the cable, bad cable, or a dirty or poor connection. Moving the connection around or replacing cables can isolate the problem.
Some number of invalid transmission words are expected and acceptable. Invalid transmission words within a frame are used to produce the bit-error threshold link incident. If one or more invalid transmission words are detected in 12 separate 1.5-second samples within 5 minutes, a bit-error threshold link incident is generated.
- **CRC errors**—A received frame failed a cyclic redundancy check (CRC) validation, indicating the frame arrived at the director's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Delimiter errors**—The number of times that the director detected an unrecognized start-of-frame (SOF), an unrecognized end-of-frame (EOF) delimiter, or an invalid class of service. This indicates that the frame arrived at the director's port corrupted. This corruption can be due to plugging/unplugging the link, bad optics at either end of the cable, bad cable, or dirty or poor connections. Moving the connection around or replacing cables can isolate the problem.
- **Address ID errors**—A received frame had an unavailable or invalid Fibre Channel destination address, or an invalid Fibre Channel source address. This typically indicates the destination device is unavailable.
- **Frames too short**—A received frame exceeded the Fibre Channel frame maximum size or was less than the Fibre Channel minimum size, indicating the frame arrived at the director's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

Operational statistics

The following describes the Operational Statistics that display for a selected port

- **Offline sequences Rx**—The number of offline sequence that the port has received.
- **Offline sequences Tx**—The number of offline sequence that the port has transmitted.
- **Link resets**—The number of link reset protocol frames received/transmitted by this port from/to the attached device. The director transmits a link reset to initiate the link reset protocol or recover from a link timeout. This occurs normally to establish BB_Credit or on any port in order to recover lost BB_Credit. The director receives a link reset from an attached device if the device wishes to initiate the link reset or recover from a link timeout.

Traffic statistics with receive and transmit values

This section describes the types of traffic statistics that display for a selected port:

- **Link Utilization % Rx** and **Link Utilization %Tx**—There are separate values for transmit (Tx) and receive (Rx) link utilization. The larger of these two values displays on the bar graph.
The current link utilization for the port is expressed as a percentage. Each port can transmit or receive data at 100 Megabytes (MB) per second if the port is set to 1 Gig. If the port is set to 2 Gig, the port can transmit or receive data at 200 MB per second. This statistic shows the percentage of the maximum link utilization currently being used. Link utilization is calculated over one-second intervals. The maximum link utilization is 100%.
- **Frames Rx**—The number of frames that the port has received.
- **Frames Tx**—The number of frames that the port has transmitted.
- **Four byte words Rx**—The number of words that the port has received.
- **Four byte words Tx**—The number of words that the port has transmitted.
- **Flows rerouted from ISL**—This displays if the optional Open Trunking feature is installed or not. A value will only display if Open Trunking is installed, the port is connected to an ISL, and flows were being rerouted. This is the number of Fibre Channel traffic flows that were rerouted from this ISL to another ISL due to congestion.
- **Flows rerouted to ISL**—This displays if the optional Open Trunking feature is installed or not. A value will only display if Open Trunking is installed, the port is connected to an ISL, and flows were being rerouted. This will be the number of Fibre Channel traffic flows that were rerouted to this ISL from another ISL due to congestion.

Using statistics for troubleshooting

As a general rule, you should clear all counts after the system is stabilized. When looking at the Performance view, roughly keep track of the time interval when errors accumulate to judge the presence and severity of a problem. Also, recognize that there is a link recovery hierarchy implemented in Fibre Channel to handle some level of *expected anomalies*. In general, only be concerned with error counts that increment very quickly.

Button functions

The two buttons located at the right end of the title bar on the **Statistics Values** table are:

- **Refresh**—Updates the data in the statistics tables and enables you to compare values at any given time. Note that you can also refresh data by clicking the port's bar graph.
- **Clear**—Clears all counters to zero. Choosing this button displays a Clear Port Statistics dialog box. Click the appropriate option button and click **OK** to clear all counters to zero on the selected port only or counters on all ports on the director. Note that this also clears counters for all Element Manager users.

An entry identifying when and by whom the statistics were cleared is saved in the **Audit Log**.

FRU List view

Display the FRU List in the View panel choosing the **FRU List** option from the view tabs. This view, as shown in [Figure 30](#), displays information about all installed FRUs on the director. All data is dynamic and updates automatically as the software detects changes.

FRU	Position	Status	Part Number	Serial Number
Backplane	0	Active	316143-001	12374878
Control Processor (CTP)	0	Active	254136-001	82372257
Control Processor (CTP)	1	Backup	316145-001	82372253
Serial Crossbar (SBAR)	0	Active	316144-001	82380004
Serial Crossbar (SBAR)	1	Backup	316144-001	82202000
Cooling Fan Module	0	Active		
Cooling Fan Module	1	Active		
Cooling Fan Module	2	Active		
Power Supply Module	0	Active	316141-001	52074128
Power Supply Module	1	Active	316141-001	52074155
G Port Module (UPM)	0	Active	292006-001	82301030
G Port Module (UPM)	1	Active	292006-001	82300772
G Port Module (UPM)	2	Active	292006-001	32473480
G Port Module (UPM)	3	Active	292006-001	32473357
G Port Module (UPM)	4	Active	292006-001	32473600
G Port Module (UPM)	5	Active	292006-001	32473349
G Port Module (UPM)	6	Active	292006-001	82301895
G Port Module (UPM)	7	Active	292006-001	82250602
G Port Module (UPM)	8	Active	292006-001	32320072
G Port Module (UPM)	9	Active	292006-001	82342010
G Port Module (UPM)	10	Active	292006-001	32473586
G Port Module (UPM)	11	Active	292006-001	32472064
G Port Module (UPM)	12	Active	292006-001	82221858
G Port Module (UPM)	14	Active	292006-001	82270485
G Port Module (UPM)	15	Active	292006-001	82300773
G Port Module (UPM)	16	Active	292006-001	82321780
G Port Module (UPM)	17	Active	292006-001	82230786
G Port Module (UPM)	18	Active	292006-001	82341759
G Port Module (UPM)	19	Active	292006-001	32473305

Figure 30 FRU List view

Information on the FRU List view for each FRU includes:

- **FRU**—A description of the FRU type, as follows:
 - **Backplane**
 - **Control Processor (CTP)**
 - **Serial Crossbar (SBAR)**

- **G Port Module**—For the fiber channel port card, the following acronyms may display to indicate the card's port technology:
 - GLSL—G_Port, long wave, single mode LC connector, 1 Gigabit
 - GSML—G_Port, short wave, multimode, LC connector, 1 Gigabit
 - GXXL—G_Port, mixed mode, LC connector, 1 Gigabit
 - FPM—G_Port, small form factor pluggable (SFP) optics, fibre port module, 1 Gigabit
 - UPM—G_Port, small form factor pluggable (SFP) optics, universal port module, 2 Gigabit
 - GSFM—G_Port, short wave, small form factor, multimode, 1 Gigabit
 - GLSR—G_Port, short wave, single mode, MT-RJ connector, 1 Gigabit
 - GXXR—G_Port, mixed mode, MT-RJ connector, 1 Gigabit
 - GXXL—G_Port, mixed mode, LC connector, 1 Gigabit
- **Cooling FAN**—Fan module.
- **PWR**—Power supply module.
- **Position**—A number representing the FRU chassis position. The chassis (slot) position for a nonredundant FRU is 0. The chassis positions for redundant FRUs are 0 and 1. For the Director 2/64 chassis, port positions are 0–63. For the Director 2/140 model, port positions are 0–127 and 132–143. Note that for the Director 2/140, ports 128–131 are internal ports and are not available for external connections.
- **Status**—The FRU status (**Active** or **Backup**).
- **Part Number**—The FRU part number.
- **Serial Number**—The FRU serial number.

To display the FRU Properties dialog box for an FRU:

- Click the FRU's row and select **Product > FRU > FRU Properties**.
- Or
- Double-click an FRU.

Port operational states

Table 4 describes the port operational states and the LED and attention indicators that display in the Hardware view and Port List view.

Table 4 Port states and indicators

Port State	Port Indicators		Alert indicator*	Description
	Green	Amber		
Beaconing	Off or On	Blink	Yellow Triangle	The port is beaconing. The amber port LED blinks once every two seconds to enable users to find a specific port. Enable beaconing through the port's menu on the Port Card view, Port List view, or Performance view.
Inactive	Off	Off	Yellow Triangle	The switch port is inactive. Reasons for this state display in the Reason field of the Port Properties dialog box. Note that if port optics have also failed, the amber LED will be on.
Invalid Attachment	On	Off	Yellow Triangle	The reasons for this state display in the Reason field of the Port Properties dialog box.
Link Incident	Off	Off	Yellow Triangle	A link incident occurred on the port. The status symbol displays in the Port List view, Port Card view, and Hardware view.
Link Reset	Off	Off	Yellow Triangle	The director and the attached device are performing a link reset operation to recover the link connection. Ordinarily, this is a transient state that should not persist.
No Light	Off	Off	None	No signal (light) is being received on the director port. This is a normal condition when there is no cable plugged into the port or when the power of the device attached to the other end of the link is off.
Not Operational	Off	Off	Yellow Triangle	The director port is receiving the Fibre Channel not operational sequence (NOS), indicating that the attached device is not operational.
Online	On	Off	None	The attached device has successfully connected to the director and is ready to communicate or is in the process of communicating with other attached devices. As long as the port remains online, the green port LED remains illuminated. Note that on the actual port in the unit, the green LED blinks when there is active Fibre Channel traffic through the port.

Table 4 Port states and indicators (continued)

	Port Indicators			
Port State	Green	Amber	Alert indicator*	Description
Offline	Off	Off	None	The director port was configured as <i>blocked</i> and is transmitting the Fibre Channel OLS to the attached device.
	Off	Off	Yellow Triangle	The director port was configured as <i>unblocked</i> and is receiving the Fibre Channel OLS, indicating that the attached device is offline.
Port Failure	Off	On	Red and Yellow Blinking Diamond	The director port has failed and requires service. The amber LED for the port remains illuminated.
Segmented E_Port	On	Off	Yellow Triangle	The E_Port is segmented preventing the two fabrics from joining (this only occurs when two directors are connected to each other). Display the Port Properties dialog box to view the segmentation reason.
Testing	Off	Blink	Yellow Triangle	Port is executing an internal loopback test.
	On	Blink	Yellow Triangle	Port is executing an external loopback test. Note: For any loopback test, the amber LED blinks (beacons) to help users locate the port under test.
Not Installed	Off	Off	None	The port optics are not installed or the feature that provides additional port function is not enabled.

* The alert indicator displays on the port in the Hardware view. It indicates that a corrective action is required to return the port to a normal operating state.


Link incident alerts

A link incident is a problem detected on a fiber-optic link, like the loss of light, invalid sequences, and other problems. When a problem occurs, a LIN alert is sent to the **Link Incident Log** in the director ElementManager. LIN alerts warn you that there is a link incident being detected through a port connection that may require operator intervention to correct.

If LIN alerts are enabled for a port in the Configure Ports dialog box, a yellow triangle (attention indicator) displays by the port connector in the Hardware view and Port Card view and in the **Alert** column in the Port List view. Double-clicking on the port in the Port Card view and Port List view with the yellow triangle displays the Port Properties dialog box.

If LIN alerts have been enabled for a port in the Configure Ports dialog box, the Port Properties dialog box contains a short description of the latest incident in the **Link Incident** field. Or, if there are no active incidents, *None* displays. The system writes all link incidents to the **Link Incident Log**.

If you enable LIN alerts for a port in the Element Manager Configure Ports dialog box, configure e-mail notification through HAFM, and enable E-Mail Notification through the Element Manager **Maintenance** menu, you will receive e-mail notification of LIN alerts.

 **NOTE:** The e-mail notification of LIN alerts is available to all users; no feature permissions are imposed.

Although you can clear the attention indicator in the Hardware view and the alert description in the Port Properties dialog box manually, they may also be cleared by actions outside of your control, such as rebooting the HAFM appliance.

You can clear the link incident indicator in the Hardware view and the description in the **Link Incident** field manually. To manually clear the attention indicator (yellow triangle), right-click the port with the yellow triangle and select **Clear Link Incident Alert(s)** from the menu. In the Clear Link Incident Alert(s) dialog box, select the appropriate option and click **OK**. Be aware that clearing the incident indicator clears it for everyone monitoring the system. If there are no link incident alerts enabled for a port, no actions occur.

Threshold alerts

A threshold alert notifies Element Manager users when the transmit (Tx) or receive (Rx) throughput reaches specific values for director ports or port types (E_Ports or F_Ports).

To display the Configure Threshold Alerts dialog box, click **Configure > Threshold Alerts**. Use this dialog box to configure criteria for generating a threshold alert.

One criteria that you must configure is a throughput value that equals a specific percentage of the port's total throughput capacity. You also provide a time interval during which throughput is measured and a time interval during which that throughput value must remain constant. When throughput reaches the threshold value and remains constant for the specified time, an alert is generated.

Threshold alerts appear in the following manner in the Element Manager:

- An attention indicator (yellow triangle) displays on the port in the Port Card view.
- An attention indicator (yellow triangle) displays on the port card in the Hardware view.
- An attention indicator (yellow triangle) displays in the **Alert** column in the Port List view.
- An attention indicator (yellow triangle) displays by the **Threshold Alerts** field in the Port Properties dialog box.
- Detailed threshold alert data displays in the **Threshold Alert Log**.

For detailed procedures to configure threshold alerts, see "[Configuring threshold alerts](#)" on page 117.

3 Configuring the director

This chapter describes how to configure your director. It also includes information about backing up and restoring configuration data.

- [Configuring identification](#), page 90
- [Configuring management style](#), page 91
- [Configuring operating parameters](#), page 91
- [Configuring switch binding](#), page 97
- [Configuring ports](#), page 97
- [Configuring port addresses \(FICON management style\)](#), page 108
- [Configuring an SNMP agent](#), page 111
- [Configuring open systems management server](#), page 113
- [Configuring FICON management server](#), page 113
- [Configuring feature key](#), page 113
- [Configuring date and time](#), page 115
- [Configuring threshold alerts](#), page 117
- [Configuring open trunking](#), page 122
- [Exporting the configuration report](#), page 122
- [Enabling Embedded Web Server](#), page 123
- [Enabling Telnet](#), page 123
- [Enabling Alternate Control Prohibited](#), page 124
- [Backing up and restoring configuration data](#), page 124

Configuring identification

Use the procedure in this section to identify the director by its name, description, location, and contact person. This information displays in the following Element Manager locations:

- Element Manager window title panel (name).
- Director Properties dialog box (name, location, contact, description).
- Identification table at the top of the Hardware view (name, location, description).

The name also displays in the director icon labels in HAFM's Physical Map/ topology if the product name is enabled through the drop-down display list on HAFM's tool bar.

Data entered through the following procedure is saved in nonvolatile random access memory (NV-RAM) on the director.

To configure identification for the director, use the following steps:

1. Click **Configure > Identification**. The Configure Identification dialog box displays.

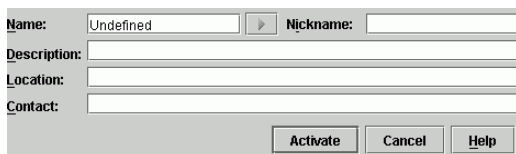



Figure 31 Configure Identification dialog box

2. Enter a name for the director in the **Name** field (24 alphanumeric characters maximum). The name could reflect the director's Ethernet network domain name service (DNS) host name, if assigned.
3. Enter a nickname for the director of up to 32 alphanumeric characters in the **Nickname** field. The nickname will display instead of the WWN in Element Manager views. (You can configure a maximum of 2,048 nicknames).


 **NOTE:** You can click the right arrow in front of this field if you want to use the name in the **Name** field as a nickname for the director's WWN. The nickname then displays instead of the WWN in Element Manager views.

4. Enter a description of the director in the **Description** field (255 characters maximum).
5. Enter the location of the director in the **Location** field (255 characters maximum).
6. Enter appropriate information about a contact person, such as a phone number, title, or e-mail address, in the **Contact** field (255 characters maximum).
7. Click **Activate** to save the data and close the dialog box.
8. If you are finished configuring the director, back up the configuration data. For more information, see "[Backup and restore configuration](#)" on page 144.

Configuring management style

To configure management style for the director, use the following steps:

1. Click **Product > Management Style** in the Element Manager window.

 **NOTE:** To change this value, you must first set the director offline.

 **NOTE:** If you change the **management style** to **FICON**, all ISL/E-Ports are disabled.

2. Click either the **Open Systems** or **FICON** option buttons:
 - Use **Open Systems** management style for all (non-FICON) Fibre Channel environments.
 - If the FICON Management Server feature is enabled, the default management style will be FICON. The management style cannot be changed to Open Systems with the FICON Management Server feature enabled. Typically, FICON management style is used when attaching an IBM FICON Parallel Enterprise or IBM zSeries server to the director and implementing inband director management through a Fibre Connection (FICON) channel.


Configuring operating parameters

Use the procedures in this section to set parameters on the director for switch and fabric operation. These operating parameters are stored in NV-RAM on the switch.

Configuring switch parameters

Use procedures in this section to set parameters on the director for switch operation through the Configure Switch Parameters dialog box.

1. Verify that the director is set offline. For instructions, see ["Set online state"](#) on page 142.

 **CAUTION:** Setting the director offline terminates all Fibre Channel connections.

2. Click **Configure > Operating Parameters > Switch Parameters**. The Configure Switch Parameters dialog box displays. [Figure 32](#) illustrates this dialog box for the Director 2/140.

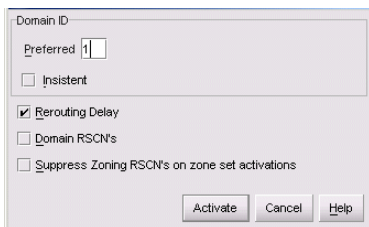


Figure 32 Configure Switch Parameters dialog box (Director 2/140)

Ordinarily, you do not need to change values in this dialog box from their defaults. The only exception is the **Preferred Domain ID**. Change this value if the director will participate in a multiswitch fabric.

1. Use information in the next section, "[Switch parameters](#)" on page 92, to change settings as required for parameters in this dialog box.
2. After you change settings, click **Activate**.
3. Set the director online. For instructions, see the "[Set online state](#)" on page 142.

Switch parameters


Configure the following parameters as required by your fabric.

Domain ID

The domain identification is a value between 1 and 31 that provides a unique identification for the switch in a fabric. A fabric switch cannot contain the same domain ID as another switch or their E_Ports will segment when they try to join.

In the Configure Switch Parameters dialog box, a field is provided to enter a preferred domain ID and a check box is provided to enable this ID as an insistent domain ID.

Preferred

 **NOTE:** To change this value, you must first set the director offline. Be sure to set the director back online after you change this value.

Use this field to set the a unique domain ID for the director. The default value is 1. Set a value between 1 and 31. When a switch comes online with a preferred ID, it requests an ID from the fabric's principal switch (indicating its preferred value as part of the request). If the requested domain ID is not allocated to the fabric, the domain ID is assigned to the requesting director or switch. If the requested domain ID is already allocated, an unused domain ID is assigned. You must set the switch or director offline before you can change the preferred domain ID.

The preferred domain ID must be unique for each director and switch in a fabric. If two directors or directors have the same preferred domain ID, the E_Ports segment, causing the fabric to segment.

For more information on domain ID, refer to the section on domain ID assignment for multiswitch fabrics in the *HP StorageWorks SAN High Availability planning guide* for details.

Insistent

This option is not operational unless the SANtegrity Binding feature is installed. Click the check box to remove or add a check mark. The default state is disabled (no check mark).

When a check mark displays, the domain ID configured in the **Preferred Domain ID** field will become the active domain identification when the fabric initializes. See the following notes:

- This option is required if Enterprise Fabric Mode (optional SANtegrity Binding feature) is enabled.
- If you enable **Insistent Domain** while the switch or director is online, the preferred domain ID will change to the current active domain ID if the IDs are different.

△ **CAUTION:** If a director with a duplicate domain ID exists in the fabric, both directors' E_Ports will segment when they try to join.

Rerouting Delay

Placing a check mark in the check box to the left of the **Rerouting Delay** option enables rerouting delay. This option is only applicable if the configured director is in a multiswitch fabric. The default state is disabled.

Enabling the rerouting delay ensures that frames are delivered in order through the fabric to their destination. If there is a change to the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.

If rerouting delay is enabled, traffic ceases in the fabric for the time specified in the **E_D_TOV** field of the Configure Fabric Parameters dialog box. This delay allows frames sent on the old path to exit to their destination before new frames begin traversing the new path.

Note that this option is required if Enterprise Fabric Mode (optional SANtegrity Binding feature) is enabled.

Domain RSCNs

Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port. Consult with your HBA and storage device vendor to determine if enabling domain RSCNs will cause problems with your HBA or storage products. For example, some hardware bus adapters (HBAs) may log out, then log back into the fabric when they receive an RSCN, thereby disrupting Fibre Channel traffic.


📅 **NOTE:** This option is required if Enterprise Fabric Mode (optional SANtegrity Binding feature) is enabled.

Suppress Zoning RSCNs on zone set activations

Fabric format domain register for state change notifications (RSCNs) are sent to ports on the switch following any change to the fabric's active zone set. These changes include activating and deactivating the zone set, or enabling and disabling the default zone. When the **Suppress Zoning RSCNs on zone set activations** check box contains a check, fabric format RSCNs are not sent for zone changes to the attached devices on the switch. Click the check box to remove or add a check mark.

This option to suppress RCNs is disabled by default and, in most cases, should be disabled so that attached devices can receive notification of zoning changes in the fabric. However, some HBAs may log out, then log back into the fabric when they receive an RSCN, thereby disrupting Fibre Channel traffic. Consult with your HBA and storage device vendor to determine if disabling this option (and thereby enabling RSCN transmission) will cause problems with your HBA or storage products.


Director Speed (Director 2/64 only)

 **NOTE:** To change this value, you must first set the director offline. Be sure to set the director back online after you change this value.

When setting the director speed, consider the following:

- Configure port speeds individually through the Configure Ports dialog box. You cannot set a director speed to less than the port speeds. If you set the director speed to 1 Gig and at least one port is configured at 2 Gig, an error message displays stating that you cannot modify the director speed.
- If you set the director data speed to 2 Gig, all installed CTP cards must support 2 Gb/s data speeds or an error message displays stating that you cannot modify the director speed.
- When you change the speed to 2 Gig, all ports on Fibre Channel port module (FPM) cards go to an inactive state. A warning/confirmation message also displays, allowing you to continue the operation or cancel. Only universal port module (UPM) cards allow 1 Gb/s and 2 Gb/s operation.
- Director firmware must support the 2 Gb/s data rate. If you set the speed to 2 Gig and the firmware only supports 1 Gb/s, an error message displays stating that the feature is not supported and providing the firmware level that will support the higher speed.

At the **Director Speed** field, click **1 Gig** or **2 Gig** to select the speed of Fibre Channel operation.

 **NOTE:** Changing the director speed to 2 Gb/s with any 1 Gb/s FPM card installed will cause the following warning/confirmation message to display: All FPM ports will be held inactive while the director is configured to 2 Gb/sec speed. Do you want to continue?

Configuring fabric parameters

Use procedures in this section to set parameters on the director for fabric operation through the Configure Fabric Parameters dialog box. These operating parameters are stored in NV-RAM on the switch.

1. Verify that the director is set offline. For instructions, see ["Set online state"](#) on page 142.

△ **CAUTION:** Setting the director offline terminates all Fibre Channel connections.

2. Click **Configure > Operating Parameters > Fabric Parameters** in the Element Manager window. The Configure Fabric Parameters dialog box displays, as shown in [Figure 33](#).

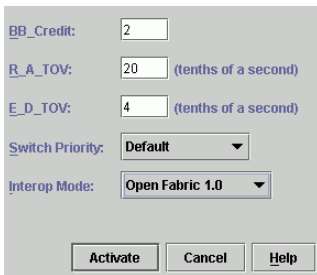


Figure 33 Configure Fabric Parameters dialog box

3. Use information in the next section, ["Fabric parameters"](#) on page 95, to change settings as required for parameters in this dialog box.
4. After you change settings, click **Activate**.
5. Back up the configuration data when you are finished configuring the director.
6. Set the director online. For instructions, see ["Set online state"](#) on page 142.

Fabric parameters


Configure the following parameters as required by your fabric.

BB_Credit

Configure the director to support buffer-to-buffer credit (BB_Credit) from 1 through 60. This will become the value used for all ports, except those configured for extended distance buffering (10–100 km). The default value is 16. For a description of the buffer-to-buffer credit, refer to industry specification, *Fibre Channel Physical and Signaling Interface*.


R_A_TOV

Configure resource allocation time-out value (R_A_TOV) in tenth-of-a-second increments. This variable works with the error detect time-out value (E_D_TOV) variable to control the director's behavior when an error condition occurs. Resources are allocated to a circuit when errors are detected and are not released for reuse until the time set by the R_A_TOV value expires. The default value is 100 tenths (10 seconds). Set a value between 10 tenths and 1200 tenths (1 through 120 seconds).

 **NOTE:** Set the same value for R_A_TOV on all directors and switches in a multiswitch fabric. If the value is not the same on all units, the fabric segments. Also, the value for R_A_TOV must be greater than the value configured for E_D_TOV.

E_D_TOV

Adjust the E_D_TOV in tenth-of-a-second increments. An error condition occurs when an expected response is not received within the time limit set by this value. The default value is 20 tenths (2 seconds). Set a value between 2 tenths through 600 tenths (.2 through 60 seconds).

 **NOTE:** Set the same value for E_D_TOV on all directors and directors in a multiswitch fabric. If the value is not the same, the fabric segments.

Switch Priority


Setting this value determines the principal director for the multiswitch fabric. Click **Principal** (highest priority), **Default**, or **Never Principal** (lowest priority) on the **Switch Priority** drop-down list.

Setting these priority values determines the principal director selected for the multiswitch fabric. For example, if you have three directors in the fabric and set one as **Principal**, one as **Default**, and one as **Never Principal**, the unit set to **Principal** becomes the principal director in the fabric.

If all directors are set to **Principal** or **Default**, the director with the highest priority and the lowest WWN becomes the principal director. Following are some examples of principal director selection when directors have these settings:

- If you have three directors and set all to **Default**, the director with the lowest WWN becomes the principal director.
- If you have three directors and set two to **Principal** and one to **Default**, the director with the **Principal** setting that has the lowest WWN becomes the principal director.
- If you have three directors and set two to **Default** and one to **Never Principal**, the director with the **Default** setting and the lowest WWN becomes the principal director.

At least one director in a multiswitch fabric needs to be set as **Principal** or **Default**. If all of the directors are set to **Never Principal**, all of the interswitch links (ISLs) will segment. If all but one director is set to **Never Principal** and the director that was principal goes offline, then all of the other ISLs will segment.

 **NOTE:** We recommend you leave the switch priority setting as Default. If you are considering setting this value to something other than default, refer to the section on principal switch selection for multiswitch fabrics in the *HP StorageWorks SAN High Availability planning guide* for details.

For example, in the audit log, you may notice that the **Principal** setting maps to a number code of 1, **Default** maps to a number code of 254, and **Never Principal** maps to a number code of 255. The number codes of 2–253 are not currently in use.

Interop mode

Select one of the following modes:


- **Homogeneous Fabric**—Select this mode if the fabric contains only HP directors and switches that are operating in Homogeneous Fabric mode.
- **Open Fabric 1.0**—Default. Select this mode if the fabric contains HP directors and switches, as well as other open-fabric compliant switches. Select this mode for managing heterogeneous fabrics.

Configuring switch binding

For complete procedures on configuring this optional feature, see [“SANtegrity features”](#) on page 159.

Configuring ports


Use the Configure Ports dialog box to configure names, blocked and unblocked state, 10–100 km extended distance buffering, enable or disable link incident (LIN) alerts for ports, port type, port speed, Port Binding, and the Bound WWN.

 **NOTE:** The **Configure Ports** dialog box is different for FICON and Open Systems management styles. Those options available in Open Systems management style only are labeled as such.

The Port Binding feature must be installed before the **Port Binding** and **Bound WWN** columns can be used. See [“Configuring open systems management server”](#) on page 113 to install the Port Binding feature.


Port configuration data is stored in NV-RAM on the switch. Configure data in the following columns of the Configure Ports dialog box:

- **Port #**—You cannot edit this field. The physical port number, from **0-63** on the Director 2/64, and **0-127** and **132-143** on the Director 2/140. Note that for the Director 2/140, ports **128-131** are internal ports and not available for external connections.
- **Name** (Open Systems management style only)—Enter a name for the port. The port names display in the Port Properties dialog box and elsewhere in the Element Manager to identify the port.

 **NOTE:** To identify port numbers for which you want to provide names, place the mouse pointer over the ports in the **Hardware view**. As you move over a port, a message displays that identifies the slot number where the port is installed.

To name ports in FICON management style, use the Configure Addresses dialog box.

- **Blocked** (Open Systems management style only)—Placing a check mark in the check boxes of this column blocks the operation of the port.
To block ports in FICON management style, use the Configure Addresses dialog box.
- **10-100Km**—This column is for extended distance buffering. You can enable extended distance for a port even if it is not an extended distance port. However, enabling extended distance buffering on a port disables the ability for the port to send broadcast traffic. When you select this option, the port can support up to 60 buffer-to-buffer credits (BB_Credits) to handle link distances up to 100 km. If this option is not enabled, the port uses the BB_Credit (1–60) configured through the Configure Fabric Parameters dialog box.
If a device is connected and logged in to the fabric when extended distance is enabled or disabled on the corresponding port, the switch will send OLS for 5 ms to force the device to log in again and obtain the new BB_Credit value set for the port.
Click **Activate** to display the 10-100Km configuration dialog box.

 **NOTE:** If a switch supports BB credits by port, an RX BB Credits column replaces the 10-100Km column.

- **RX BB Credit**—If a director supports BB credits by port, this column displays instead of the 10-100 Km column. Minimum and maximum allowable port BB credit values vary by switch. If an invalid value is entered, an Invalid RX BB Credit error message displays. The BB credit value cannot be changed unless the port is offline. The BB Credit value is validated as entered. Click **Activate** to display the RX-BB Credit Confirmation box.
In addition to the maximum BB credit limit per port, the total BB credits allocated to all ports cannot exceed the buffer pool size.

NOTE: Only 24-Port switches have a switch-wide buffer pool. The Configure Ports dialog box displays the total and available buffers at the bottom of the dialog box. When information is changed in the RX BB Credit column, this information also updates. If information is entered that exceeds the buffer pool and **Activate** is clicked, an error message displays. Also, ports for the 24-Port switches can be individually configured between 2-12, with a total number of port credits of 150.

Right-clicking in the RX-BB Credit column displays a RX BB Credits dialog box. For switches without buffer pools, this dialog box allows you to **Set all**. Set all sets all ports to a single value or **Set all to maximum** which set all ports to a maximum BB credit value. For switches with buffer pools, this dialog box allows you to **Set all**, which sets all ports to a single value or to **Distribute** which evenly distributes the pool buffers among all ports. Clicking **OK** changes the values in the Configure Port dialog box. Clicking **Activate** changes the values on the Switch.

Clicking **Set all** displays the Set All RX BB Credits dialog box. Entering a value for RX BB Credit and clicking **OK** propagates the value to all ports on the Configure Ports dialog box. If an invalid value is entered, a message dialog box displays.

- **LIN Alerts**—A link incident (LIN) is a problem detected on a fiber optic link, such as the loss of light or invalid sequences. When a problem occurs, a LIN alert is sent to the Link Incident Log in the switch Element Manager. LIN alerts warn you that there is a link incident being detected through a port connection.

Place or remove check marks in the check boxes in this column to enable or disable link incident alerts. The factory default is to enable LIN alerts.


A link incident causes a yellow attention indicator (triangle) to display for the port in the Hardware view, Port Card view, and in the **Alert** column of the Port List view. Once a LIN occurs, you must acknowledge it by choosing the Clear Link Incident Alert option from the right-click menu for the port (Hardware view). A description of the alert displays in the **Link Incident** field of the Port Properties dialog box (see [Figure 23](#) on page 65).

If the check boxes in this column are not selected, no link incident indicators display in the Hardware view. Also, the **Link Incident** field of the Port Properties dialog box is blank and a link incident is recorded in the **Link Incident Log**. LINs are always logged in the **Link Incident Log**, regardless of the configuration.

If LIN Alerts are enabled, you can receive e-mail notification when a LIN occurs. To receive e-mail notification, you must configure and enable this feature in the **Maintenance** menu of the StorageWorks HA-Fabric Manager (HAFM) and enable e-mail notification through the Enable E-Mail Notification option in the Element Manager's **Maintenance** menu.


For additional information about LIN alerts, see "[Link incident alerts](#)" on page 87.

- **Type**—Select each port's type (**G_Port**, **E_Port**, or **F_Port**) in this column from the drop-down list.

 **NOTE:** If director firmware level is below 6.0 and FICON management style is enabled, you cannot change port types unless the optional SANtegrity Binding feature is installed. If ports are configured as E_Ports in Open Systems management style, and you install SANtegrity Binding before changing to FICON management style, the ports will remain as E_Ports when you change to FICON management style. If SANtegrity Binding is not installed, setting a director to FICON management style will change all E_ports to G_Ports.

- **Port Binding**—Placing a check mark in the check boxes of this column enables the Binding state of the port.
- **Speed**—Click the **Speed** column for a specific port, and then click **2 Gig**, **1 Gig**, or **Negotiate**. This sets the data rate for the port. Choosing **Negotiate** allows the port to negotiate the data speed with an attached device. Follow this rule when setting the data speed:
 - Only set the speed to **2 Gig** on ports that support this speed. If the port optics do not support 2 Gig, a warning displays stating that the optical transceiver in the port does not support the data rate.
 - Do not set the port speed greater than the director speed. For example, if you set the port speed to **2 Gig** and the director data speed is set to **1 Gig**, an error displays stating that port speeds cannot be configured at higher data rates than the director speed. The director speed is set through the Configure Operating Parameters dialog box (Director 2/64 only).

When you change a port's speed and click **Activate** on the dialog box, a confirmation message displays stating that this setting will temporarily disrupt port data transfers.

 **NOTE:** Your director model, firmware, and port cards may not allow 2 Gig data speeds.

- **Bound WWN**—Enter the WWN or nickname of the device that is attached to the port.
If the check box in the **Port Binding** column is checked and a WWN is entered in the **Bound WWN** field, only the specified device can attach to the port.
If the check box in the **Port Binding** column is checked but no WWN is entered in the **Bound WWN** field, no device can connect to the port.
If the check box in the **Port Binding** column is not checked, any device can connect to the port (provided that the port type matches and the check box in the **Blocked** column is not checked). Any WWN or nickname entered in the **Bound WWN** field is stored.
When you click **Activate**, if the check box in the **Port Binding** column is checked and the WWN or nickname in the **Port Binding** column does not match the device actually connected to the port, the warning dialog box displays. If you click **Continue**, the currently attached devices are logged off.

Warnings and error messages


If you click **Activate** when any node attached to a port does not match the WWN or nickname in that port's **Bound WWN** column, a Warning! dialog box displays. If you click **Continue**, all nodes listed will be logged off, and the ports will attach to the respective devices identified in the **Bound WWN** column.

If you click **Activate** when the format for the WWN or nickname in the **Bound WWN** column is not valid, an error message displays. For example, The WWN is not in the `xx.xx.xx.xx.xx.xx.xx.xx` format.

Menu options

Menu options are available when you right-click any column except the **Port #** column:

- **Name** (Open Systems management style only)
 - **Clear All Port Names**—Clears all port names entered in this column.
- **Blocked (open systems management style only)**
 - **Block All Ports**—Places a check mark in all check boxes in the **Blocked** column and blocks all ports on the switch.
 - **Unblock All Ports**—Clears all check boxes in the **Blocked** column and unblocks all ports on the switch.
- **10-100 km**
 - **Clear All 10-100 km**—Clears all check boxes in the column. No port will be set for extended distance buffering.
 - **Set All 10-100 km**—Places a check mark in all check boxes in the column and sets extended distance buffering for all ports.
- **LIN Alerts**
 - **Clear All LIN Alerts**—Clears all **LIN Alert** check boxes in the column. LIN alerts will be disabled for all ports on the switch.
 - **Set All LIN Alerts**—Places a check mark in all check boxes in this column. LIN alerts will be enabled for all ports on the switch.
- **Type (open systems management style only)**
 - **Set All to G_Ports**—Sets all fields in this column to **G_Port** and configures all ports on the switch as G_Ports.
 - **Set All to F_Ports**—Sets all fields in this column to **F_Port** and configures all ports on the switch as F_Ports.
 - **Set All to E_Ports**—Sets all fields in this column to **E_Port** and configures all ports on the switch as E_Ports.
- **Speed**
 - **Set All To 1 Gb/sec**—Sets the port optics to a 1 Gb/s data rate.
 - **Set All To 2 Gb/sec**—Sets the port optics to a 2 Gb/s data rate.
 - **Set All To Negotiate**—Allows the port to negotiate the data rate with the attached device.

 **NOTE:** Your director model, firmware, and port cards may not allow 2 Gb/s data speeds.

- **Port Binding**

- **Bind All WWNs**—Places a check mark in all check boxes in this column and binds each port to the device with the WWN or nickname entered in the **Bound WWN** column for that port.
- **Unbind All WWNs**—Removes check marks in all check boxes in this column. A device with any WWN can attach to all ports.
- **Bind All Ports to Attached WWN**—Places a check mark in all check boxes in this column and binds each port to the device currently attached to that port. The **Bound WWN** column will display that device's WWN.
- **Bind Port to Attached WWN**—Places a check mark in the check box for the port where you clicked to display the menu. This binds that port to the device currently attached to that port. The **Bound WWN** column will display that device's WWN.
- **Clear All Bound WWNs**—Clears all WWNs listed in the **Bound WWN** column.

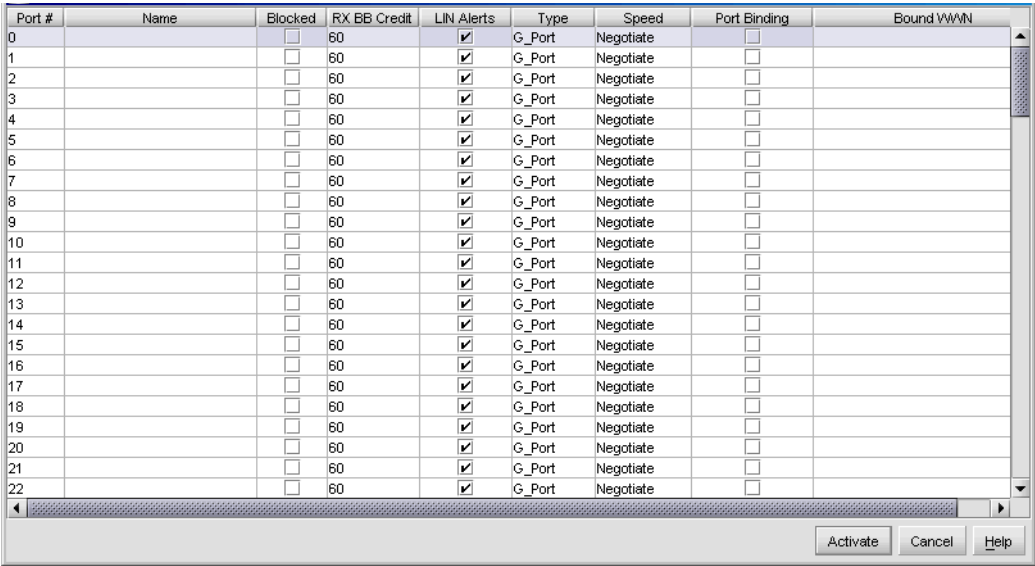
- **Bound WWN**

- **Bind All WWNs**—Places a check mark in all check boxes in this column and binds each port to the device with the WWN or nickname entered in the **Bound WWN** column for that port.
- **Unbind All WWNs**—Removes check marks in all check boxes in this column. A device with any WWN can attach to all ports.
- **Bind All Ports to Attached WWN**—Places a check mark in all check boxes in this column and binds each port to the device currently attached to that port. The **Bound WWN** column will display that device's WWN.
- **Bind Port to Attached WWN**—Places a check mark in the check box for the port where you clicked to display the menu. This binds that port to the device currently attached to that port. The **Bound WWN** column will display that device's WWN.
- **Clear All Bound WWNs**—Clears all WWNs listed in the **Bound WWN** column.

Configuring ports (Open Systems management style)

To configure ports in Open Systems management style, use the following steps:


- 1. Click **Configure > Ports** on the Element Manager menu bar. The Configure Ports dialog box displays, as shown in Figure 34.



Port #	Name	Blocked	RX BB Credit	LIN Alerts	Type	Speed	Port Binding	Bound VMMN
0		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
1		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
2		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
3		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
4		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
5		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
6		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
7		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
8		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
9		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
10		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
11		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
12		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
13		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
14		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
15		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
16		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
17		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
18		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
19		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
20		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
21		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
22		<input type="checkbox"/>	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	

Figure 34 Configure Ports dialog box (Open Systems management style)

Ports are numbered from 0–63 on the Director 2/64, and 0–127 and 132–143 on the Director 2/140.

 **NOTE:** Director 2/140, ports 128–131 are internal ports and not available for external connections.

- 2. Type a name that reflects the end device connected through the port in the **Name** field. For example, use `XYZ Server`, where `XYZ` is the brand name of the server.
- 3. Click the check box in the **Blocked** column to block or unblock operation for a port.
- 4. Click the check box in the **10-100 km** column to enable or disable extended distance buffering for the port.
- 5. If a director supports BB Credit, the **RX BB Credit** column replaces the **10-100km** column. Use this to set minimum and maximum allowable port BB credit values as follows:

- a. Right-click in the RX-BB Credit column to display the RX BB Credits dialog box as shown in Figure 35:

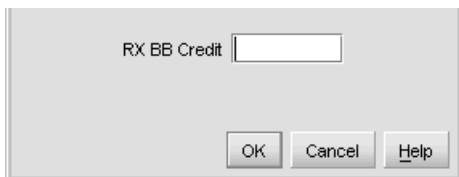



Figure 35 RX BB Credit dialog box

Set the values as follows:

- For switches without buffer pools, use **Set all** to set all ports to a single value or **Set all to maximum**, which set all ports to a maximum BB credit value.
 - For switches with buffer pools, this dialog box allows you to **Set all**, which sets all ports to a single value or select **Distribute**, which evenly distributes the pool buffers among all ports.
- b. Confirm your changes:
- Clicking **OK** changes the values in the Configure Port dialog box.
 - Clicking **Activate** changes the values on the director.
6. Click the check box in the **LIN Alerts** column to enable or disable LIN alerts for the port.

 **NOTE:** The factory default for LIN alerts is enabled.


7. Click the **Type** field to select a port type.
8. Click the check box in the **Port Binding** column to prevent an unspecified device from being connected to the port when you.
9. Click in the **Speed** column for the port and click **1 Gig**, **2 Gig**, or **Negotiate** to set the data speed for the port. When you click **Negotiate**, it allows the port and attached device to negotiate the data rate.

 **NOTE:** Your director model, firmware, and port card may not allow 2 Gb/s data speeds.

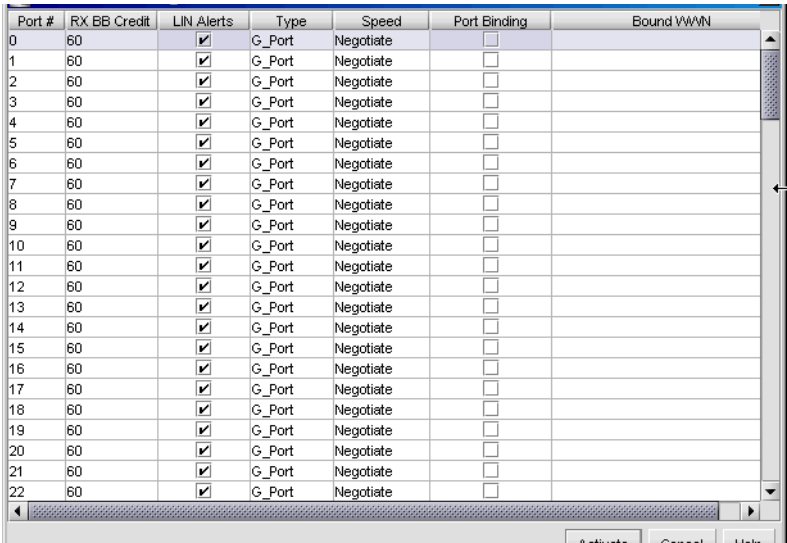
10. Click the **Bound WWN** field and enter the WWN or nickname of the specific device to be connected to the port.
11. Use the scroll bar on the right side of the Configure Ports dialog box table to display additional ports that you want to configure.
12. Click **Activate** to activate the changes and close the dialog box.
13. If you are finished configuring the switch, back up the configuration data. For more information, see ["Backing up and restoring configuration data"](#) on page 124.

Configuring ports (FICON management style)

To configure ports in FICON management style, use the following steps:

 **NOTE:** You cannot configure port names in the **Configure Ports** dialog box in FICON management style. Use the **Configure Addresses - "Active"** dialog box.

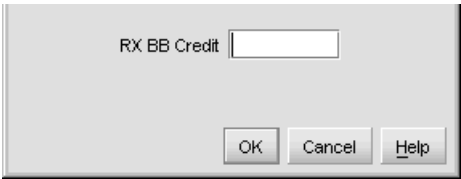
1. Click **Configure > Ports** on the menu bar. The Configure Ports dialog box displays, as shown in Figure 36.



Port #	RX BB Credit	LIN Alerts	Type	Speed	Port Binding	Bound VVWN
0	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
1	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
2	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
3	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
4	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
5	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
6	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
7	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
8	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
9	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
10	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
11	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
12	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
13	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
14	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
15	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
16	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
17	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
18	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
19	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
20	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
21	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	
22	60	<input checked="" type="checkbox"/>	G_Port	Negotiate	<input type="checkbox"/>	

Figure 36 Configure Ports dialog box (FICON management style)

- Ports are numbered from 0-63 on the Director 2/64, and 0-127 and 132-143 on the Director 2/140. Note that for the Director 2/140, ports 128-131 are internal ports and not available for external connections.
2. Click the check box in the **10-100 km** column to enable or disable extended distance buffering for the port.
 3. If a director supports BB Credit, the **RX BB Credit** column replaces the **10-100km** column. Use this to set minimum and maximum allowable port BB credit values as follows:
 - a. Right-click in the RX-BB Credit column to display the RX BB Credits dialog box as shown in Figure 37:



RX BB Credit

OK Cancel Help

Figure 37 RX BB Credit dialog box

Set the values as follows:

- For switches without buffer pools, use **Set all** to set all ports to a single value or **Set all to maximum**, which set all ports to a maximum BB credit value.
 - For switches with buffer pools, this dialog box allows you to **Set all**, which sets all ports to a single value or select **Distribute**, which evenly distributes the pool buffers among all ports.
- b. Confirm your changes:
- Clicking **OK** changes the values in the Configure Port dialog box.
 - Clicking **Activate** changes the values on the director.
4. If a director supports BB Credit, the **RX BB Credit** column replaces the **10-100km** column. Use this to set minimum and maximum allowable port BB credit values:
- a. Right-click in the RX-BB Credit column to display the RX BB Credits dialog box as shown in Figure 38:

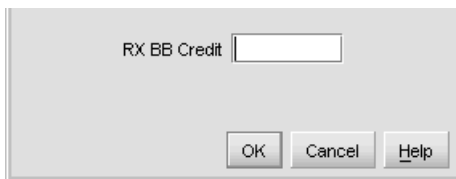


Figure 38 RX BB Credit dialog box

Set the values as follows:

- For switches without buffer pools, use **Set all** to set all ports to a single value or **Set all to maximum**, which set all ports to a maximum BB credit value.
 - For switches with buffer pools, this dialog box allows you to **Set all**, which sets all ports to a single value or select **Distribute**, which evenly distributes the pool buffers among all ports.
- b. Confirm your changes:
- Clicking **OK** changes the values in the Configure Port dialog box.
 - Clicking **Activate** changes the values on the director.
5. Click the check box in the **LIN Alerts** column to enable or disable LIN alerts for the port.



NOTE: The factory default for LIN alerts is enabled.

6. Click the check box in the **Port Binding** column to prevent an unspecified device from being connected to the port.
7. Click in the **Speed** column for the port and click **1 Gig**, **2 Gig**, or **Negotiate** to set the data speed for the port. When you click **Negotiate**, it allows the port and attached device to negotiate the data rate.



NOTE: Note that your director model and firmware may not allow 2 Gb/s data speeds.

8. Click the **Bound WWN** field and enter the WWN or nickname of the specific device to be connected to the port.
9. Use the scroll bar on the right side of the Configure Ports dialog box table to display additional ports that you want to configure.
10. Click **Activate** to activate the changes and close the dialog box.
11. If you are finished configuring the switch, back up the configuration data. For more information, see ["Backing up and restoring configuration data"](#) on page 124.


Configuring port addresses (FICON management style)

This procedure applies only to a director that is using FICON Management Style. Use this procedure to create and activate port address configurations in the Configure Address - "Active" dialog box (see [Figure 40](#) on page 109.)

Parameters

- **Addr**—This read-only field lists the port's address. Each port in the switch has a corresponding port address which equals the physical port number plus four. Therefore, the address for port 0 is 4 (0+4).
- **Port Name**—This user-defined name is assigned to the address. Up to 24 alphanumeric characters are allowed, including spaces, hyphens, and underscores.
- **Blocked**—If the box is checked, the port is blocked. Blocked ports continuously transmit offline sequences (OLS), but cannot communicate to an attached device. If the box is not checked, the port is unblocked.
- **Port connection array**—This yellow area of the dialog box is a matrix of port addresses that is used to configure connections between port addresses.

All port addresses for the director are listed along the top and left side of the matrix. To allow or prohibit connections between two addresses, click the cell at the intersection of a vertical and horizontal row of cells. Right-click the intersecting cell to display a menu of attributes.

 **NOTE:** For the Director 2/140, port addresses 84–87 contain Xs. These refer to the internal ports 128–131, which cannot have external fiber cable connections.

The default state of a cell is an empty cell (square), which represents an allowed connection. The symbol for a prohibited connection is shown in [Figure 39](#). Click a cell to add the prohibited symbol and prohibit connection to that cell. To remove the prohibit symbol, click the cell again.



Figure 39 Prohibited Port connection symbol

Move your mouse pointer over the squares in the array to display the corresponding address. Right-click the array to display the following menu options:

- **Prohibit row**—Prohibits connection between all addresses in a row. In effect, this prohibits connection between a specific address and all other port addresses.
- **Allow row**—Allows connection for all port addresses on a row that are currently prohibited. This allows connection between a port with a specific address and other allowed ports.
- **Prohibit all**—Prohibits connection between all port addresses. In this state, ports in the switch cannot connect with any other port address.
- **Allow all**—This allows a dynamic connection through all port addresses from which connection is currently prohibited. The allowed attribute has the lowest precedence and does not override any other attribute.

- **Block all ports**—Blocks communication between all ports. Ports that are blocked continuously transmit offline sequences (OLS).
- **Unblock all ports**—Unblocks all port addresses that are currently blocked. This allows communication from all port addresses in the switch.
- **Clear all**—Clears the prohibit and blocked status of all port addresses in the switch.
- **CUP Name**—This user-defined name is assigned to the control unit port (CUP). Up to 24 alphanumeric characters allowed, including spaces, hyphens, and underscores. A space is not allowed as the first character, and the characters are case-sensitive. This is not a required field.
- **Activate**—Click to activate the current configuration. A warning displays before the action occurs.
- **Save As**—Click to save the current configuration with a name and description. The saved configuration will be stored on the HAFM appliance and in the Address Configuration Library. See “[Managing stored address configurations \(FICON management style\)](#)” on page 110” for information on accessing this library.
- **Cancel**—Click to cancel the configuration settings and close the dialog box without saving. If you click this button after you click **Save As**, your changes will be saved and the dialog box will simply close.

Configure port addresses procedure

To configure, save, and activate port addresses, use the following steps:

1. Click **Configure > Addresses** on the menu bar, then click **Active**. The Configure Addresses - “Active” dialog box displays.

Addr	Port Name	Blocked	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13
04		<input checked="" type="checkbox"/>									⊗							
05		<input type="checkbox"/>				⊗					⊗							
06		<input type="checkbox"/>									⊗							
07		<input type="checkbox"/>		⊗							⊗							
08		<input type="checkbox"/>									⊗							
09		<input checked="" type="checkbox"/>									⊗							
0A		<input type="checkbox"/>									⊗							
0B		<input type="checkbox"/>									⊗							
0C		<input type="checkbox"/>	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗
0D		<input type="checkbox"/>									⊗							
0E		<input checked="" type="checkbox"/>									⊗							
0F		<input type="checkbox"/>									⊗							
10		<input type="checkbox"/>									⊗							
11		<input type="checkbox"/>									⊗							
12		<input type="checkbox"/>									⊗							
13		<input checked="" type="checkbox"/>									⊗							
14		<input type="checkbox"/>									⊗							


CUP Name:

☐ Active-Saved

Figure 40 Configure Addresses - “Active” dialog box

2. Enter information into the appropriate fields.

3. Click the squares to either prohibit or allow connections.
In [Figure 40](#) on page 109, port address 07 is prohibited from communicating with port address 05. Also, Port OC is prohibited from communicating with all other port addresses.
4. Click **Save As** to open the Save Address Configuration As dialog box.
5. Click the **Port Name** field and enter a name.
Names must be between 1 and 8 characters in length. Valid characters are uppercase A–Z, 0–9, hyphen (-), and underscore (_). The name may not be CON, AUX, COMn (where n=1-9), LPTn (where n=1-9), NUL, or PRN.
Descriptions must be between 0 and 24 characters in length. Up to 24 alphanumeric characters allowed, including spaces, hyphens, and underscores.
6. Click **OK** to save changes and to close the Save Address Configuration As dialog box.
7. In the Configure Addresses - “Active” dialog box, click **Activate** to activate the configuration or click **Cancel** to close without activating.

 **NOTE:** If you click **Cancel** after saving, your configuration will still be added to the library without being activated.

Managing stored address configurations (FICON management style)

This procedure applies only to a director that is using FICON Management Style.

Once address configurations are created through the Configure Addresses - “Active” dialog box, they are saved to the **Address Configuration Library**. Use this procedure to manage address configurations in the **Address Configuration Library**.

To manage saved library entries:

1. Click **Configure > Addresses** on the menu bar and then click **Stored**. The Address Configuration Library dialog box displays, as shown in [Figure 41](#).

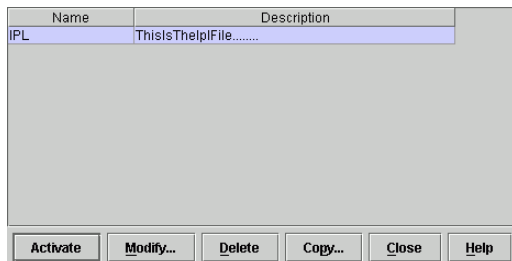



Figure 41 Address Configuration Library dialog box

2. Select a configuration entry by selecting a row. Then use one of the procedures below.
 - Click **Modify** to modify a stored configuration. The Configure Addresses dialog box displays for the configuration. See “[Configuring port addresses \(FICON management style\)](#)” on page 108 for details on using this dialog box.
 - Click **Delete** to delete a stored configuration. A warning displays before deletion.

- Click **Copy** to copy a stored configuration. When the Copy Address Configuration dialog box displays, provide a name and description for the configuration.
- Names must be between 1 and 8 characters in length. Valid characters are uppercase A–Z, 0–9, hyphen (-), and underscore (_). The name may not be CON, AUX, COMn (where n=1-9), LPTn (where n=1-9), NUL, or PRN. Descriptions must be between 0 and 24 characters in length. Up to 24 alphanumeric characters are allowed, including spaces, hyphens, and underscores. Click **OK** and the configuration is added to the library.
- Click **Activate** to activate a stored configuration and send it to the switch for immediate use. A warning displays before the action occurs.


 **NOTE:** If **Active=Saved** is enabled through the **Configure FICON Management Server** dialog box, this overwrites the current IPL address configuration.

3. Click **Close** to close the dialog box when you are finished managing the library.


Configuring an SNMP agent

Use the procedures in this section to:

- Configure the SNMP agent that runs on the director and implements the following MIBs:
 - MIB-II
 - Fibre Channel Fabric Element MIB
 - Director private MIB
 - Fibre Alliance MIB

 **NOTE:** For complete information on objects defined in MIBs and steps to download MIB variables to your SNMP workstation, refer to the *HP StorageWorks SNMP reference guide for Directors and Edge Switches*.

- Configure network addresses and community names for up to six SNMP trap recipients. An SNMP trap recipient is a network management station that receives messages through SNMP for specific events that occur on the director.
- Define SNMP community names that SNMP managers use for reading variables.
- Authorize write permissions for writable MIB variables.

 **NOTE:** SNMP managers may request, but will not receive, traps and SNMP data through SNMP management stations that are not configured with community names.

To configure the SNMP agent:

1. At the Hardware view page, click **Configure > SNMP Agent**. The Configure SNMP dialog box displays, as shown in [Figure 42](#) on page 112.
 - a. For each trap recipient to be configured, type a community name of 32 or fewer alphanumeric characters in the associated **Community Name** field. The community name is incorporated in SNMP trap messages to ensure against unauthorized viewing or use.
 - b. Click the check box in the **Write Authorization** column to enable or disable write authorization for the trap recipient (default is disabled). A check mark in the box indicates write authorization is enabled. When the feature is enabled, a management workstation user can change the HAFM appliance's **sysContact**, **sysName**, and **sysLocation** SNMP variables.
 - c. Select the Fibre Alliance MIB version supported on the director by clicking the drop-down list in the top right corner of the dialog box. Selections are 3.0 and 3.1.
 - d. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the associated **Trap Recipient** field. Use 64 or fewer alphanumeric characters. Hewlett-Packard recommends using the IP address.

Community Name	Write Authorization	Trap Recipient	UDP Port Number
community sys	<input checked="" type="checkbox"/>	79.784.331	
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		

Activate Cancel Help

Figure 42 Configure SNMP dialog box

- e. Type a decimal user datagram protocol (UDP) port number in the associated **UDP Port Number** field. (This number is commonly 162.)
2. Click the **Enable Snmp Agent** check box to enable the agent on this director.
3. Click the **Enable Authorization Traps** check box to enable authorization trap messages to be sent to SNMP management stations when unauthorized stations try to access SNMP information from the director.
4. Click the **Fibre Alliance MIB Version** drop-down list to select the Fibre Alliance MIB version supported on the director.
5. Click **Activate** to save the information and close the dialog box.
6. If you are finished configuring the director, back up the configuration data. For more information, see ["Backup and restore configuration"](#) on page 144.

Configuring open systems management server

For complete procedures on configuring this optional feature, see “[Configuring the open systems management server](#)” on page 159.


Configuring FICON management server

For complete procedures on configuring this optional feature, see “[Configuring the FICON management server](#)” on page 156.

Configuring feature key

Feature keys verify ownership of the Element Manager and optional features that can be purchased for the Element Manager. The feature key, which is encoded with a director’s serial number, can only be configured on the director to which it is assigned.

A feature key is a string of alphanumeric characters consisting of both uppercase and lowercase. The following is an example of a feature key format: XxXx-XXxX-xxXX-xX.

 **NOTE:** The total number of characters may vary. The key is case sensitive and it must be entered exactly, including the dashes.

The feature key, which is encoded with a director’s serial number, can only be configured on the director to which it is assigned.

You can enable the feature key with the director online. However, if a current feature is disabled by activating a new feature key, you must take the director offline before enabling the new feature key.

Display the Configure Feature Key dialog box by choosing **Features** from the **Configure** menu on the menu bar.

FICON Management Server Feature: If you are enabling the FICON Management Server feature, the management style automatically configures to FICON management style. You cannot change the management style to Open Systems management style while the FICON Management Server feature is enabled.

To configure a feature key, use the following steps:

1. Click **Configure > Features** on the Element Manager menu bar. The Configure Feature Key dialog box displays, as shown in [Figure 43](#).

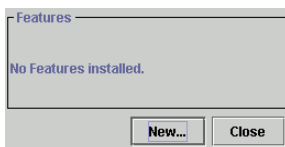


Figure 43 Configure Feature Key dialog box

2. Click **New** to add a new feature key. The New Feature Key dialog box displays, as shown in Figure 44.



Figure 44 New Feature Key dialog box

3. Enter the director's feature key in the **Key** field and click **OK**.
 - Feature keys are only valid for a director with a specific serial number. They cannot be interchanged between directors. If an error stating `Invalid serial number` displays, verify that you have entered the feature key that was assigned to the director. To verify, check the serial number of the director through the Switch Properties dialog box and compare it to the serial number listed in the documentation provided with your feature key.
 - The feature key is a string of alphanumeric characters with dashes. The key is case-sensitive, so enter the key exactly as printed in the documentation that you received for the feature. If an error stating `Invalid feature key` displays, verify that you have entered the feature key correctly.

The Enable Feature Key dialog box displays as shown in Figure 45 with a warning, stating that this action will override the current set of features on the director. The list in the left column of the dialog box is a list of features that are active on the director. The list on the right is a set of features that come with the new feature key. All of the features that are active are included in the new feature list.

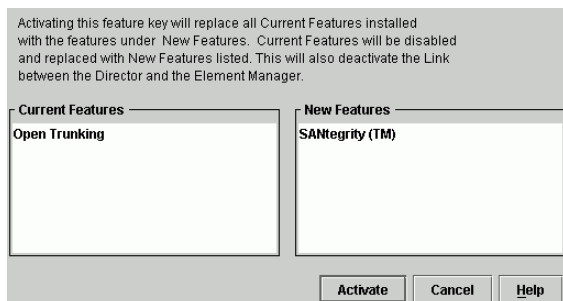



Figure 45 Enable Feature Key dialog box

4. Click **Activate** to activate the new feature key.

An IPL will occur, during which the Ethernet connection between the HAFM appliance and director is momentarily interrupted.

 **NOTE:** If you click Activate, all current features will be replaced with new features. That is, if there are features shown in the current list that are not shown in the new list, then those features will be removed from the director.

5. When you are finished configuring the director, you can back up the configuration data. For more information, see ["Backing up and restoring configuration data"](#) on page 124.

 **NOTE:** For detailed descriptions of features that you can enable using the Configure Feature Key dialog box, see ["Optional features"](#) on page 149.

No Feature Key dialog box

If you attempt to access a feature for which a feature key was not enabled, a No Feature Key dialog box displays as shown in [Figure 46](#).

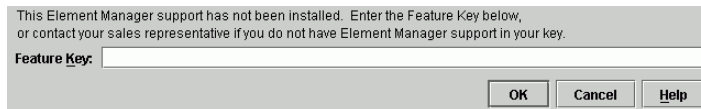



Figure 46 No Feature Key dialog box

At this point, you must enter the Element Manager feature key. After you enter a valid feature key, the Enable Feature Key dialog box displays.

Click **Activate** on the Enable Feature Key dialog box to activate the new feature key. An IPL will occur, during which the Ethernet connection between the HAFM appliance and director is momentarily interrupted. This will not disrupt Fibre Channel traffic.


 **NOTE:** If you click **Activate**, all current features will be replaced with new features. That is, if there are features shown in the current list that are not shown in the new list, then those features will be removed from the switch or director.

Because the switch or director is placed offline when you activate the Element Manager feature key, the Element Manager will not launch until it comes back online and you either:

- Right-click the switch or director and select Element Manager.
- Select the switch or director and click the Launch Element Manager icon from the tool bar.

Configuring date and time

The Director Element Manager log entries are stamped with the date and time received from the director. Use these steps to set the effective date and time for the director.

 **NOTE:** If both switch clock alert mode is enabled (only possible if FICON Management Server is enabled) and periodic synchronization is enabled, an error will result. Disable one of the modes to fix the error. See the following procedure to disable periodic synchronization. See ["Configuring FICON management server"](#) on page 113 to disable switch clock alert mode.

1. Click the **Configure > Date/Time**. The Configure Date and Time dialog box displays, as shown in [Figure 47](#).

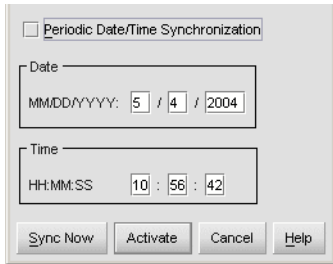


Figure 47 Configure Date and Time dialog box

2. Set director date and time manually, or set for periodic updates. For specific instructions, see the following sections:
 - ["Setting date and time manually"](#)
 - ["Synchronizing date and time"](#)

Setting date and time manually

Use these steps to set the director date and time manually.

1. At the Configure Date and Time dialog box, click the **Periodic Date/Time Synchronization** check box to deselect the option (no check mark in the box). The grayed-out **Date** and **Time** fields activate.
2. Click the **Date** fields that require change, and type numbers in the following ranges:
Month (MM): 1 through 12
Day (DD): 1 through 31
Year (YYYY): greater than 1980
3. Click the **Time** fields that require change, and type numbers in the following ranges:
Hour (HH): 0 through 23
Minute (MM): 0 through 59
Second (SS): 0 through 59
4. Click **Activate** to set the director date and time, and close the Configure Date and Time dialog box.

Synchronizing date and time

Use these steps to set the director to periodically synchronize date and time with HAFM.

1. At the Configure Date and Time dialog box, click the **Periodic Date/Time Synchronization** check box. The **Date** and **Time** fields are grayed-out and not selectable.

2. Select one of the following two options:
 - Click **Activate** to enable synchronization and close the Configure Date and Time dialog box. The director date and time synchronize with the HAFM date and time at the next update period (at least once daily).
 - Click **Sync Now** to synchronize the director and HAFM immediately. The Date and Time Synced dialog box displays.
 - Click **OK**.
 - In the Configure Date and Time dialog box, click **Activate** to enable synchronization and close the Configure Date and Time dialog box.

Configuring threshold alerts

A threshold alert notifies users when the transmit (Tx) or receive (Rx) throughput reaches specified values for specific director ports or port types (E_Ports or F_Ports). You are notified of a threshold alert by:

- A yellow triangle that displays on the port in the Port Card view.
- A yellow triangle that displays on the port in the Hardware view.
- A yellow triangle that displays in the **Alert** column of the Port List view.
- A yellow triangle that displays by the **Threshold Alerts** field in the Port Properties dialog box.
- Detailed threshold alert data recorded in the **Threshold Alert Log**.


Use the **Threshold Alerts** option on the **Configure** menu to configure the following:

- Name for the alert.
- Type of threshold for the alert (Rx, Tx, or either).
- Active or inactive state of the alert.
- Threshold criteria:
 - Percent traffic capacity utilized—The percent of the port's throughput capacity achieved by the measured throughput. This setting constitutes the threshold value. For example, a value of 50 means that the port's threshold is reached when throughput is 50% of capacity.
 - Time interval during which throughput is measured and alert notification can occur.
 - The maximum cumulative time that the throughput percentage threshold can be exceeded during the set time interval before an alert is generated.
- Ports for which you are configuring threshold alerts.

You can configure up to 16 alerts, and any number of alerts can be active at one time. Use the following procedures to create a new threshold alert or to modify, activate, deactivate, or delete an alert.

Creating new alerts

1. In the Hardware view, click **Configure > Threshold Alerts**. The Configure Threshold Alert(s) dialog box displays, as shown in [Figure 48](#) on page 118.

 **NOTE:** If alerts are configured, they will display in table format showing the name of the alert, type of alert (Rx, Tx, or Rx or Tx), and alert state (inactive or active).

Name	Type	State
90 alert	Receive And Transmit	Active
test 2	Receive And Transmit	Inactive
test threshold	Receive And Transmit	Inactive

New...

Modify...

View

Delete

Activate

Deactivate

Close

Help

Figure 48 Configure Threshold Alert(s) dialog box

2. Click **New**. The New Threshold Alert dialog box displays, as shown in [Figure 49](#).

Enter name and type of threshold alert:

Threshold Alert Name:

Threshold Type:

Select One

<< Previous

Next >>

Finish

Cancel

Help

Figure 49 New Threshold Alerts dialog box - first screen

3. Enter a name from one to 64 characters in length. All characters in the ISO Latin-1 character set, excluding control characters, are allowed.
4. Click one of the following on the drop-down list under the **Name** field:
 - **Rx Throughput**—An alert will occur if the threshold set for receive throughput is reached

- **Tx Throughput**—An alert will occur if the threshold set for transmit throughput is reached.
 - **Rx or Tx Throughput**—An alert will occur if the threshold set for either receive or transmit throughput is reached.
5. Click **Next**. A new screen displays with additional parameters, as shown in [Figure 50](#). The name configured for the alert displays at the top of the screen.



NOTE: Click **Previous** if you need to return to the previous screen.

Figure 50 New Threshold Alerts dialog box - second screen

6. Enter a percentage from 1 through 100 for **% utilization**. When throughput reaches this percentage of port capacity, a threshold alert will occur.
7. Enter the amount of cumulative minutes in which the % utilization should exist during the notification interval before an alert is generated. You can also click **At any time** if you want an alert to occur whenever the set % utilization is reached. The valid range is from 1 to the interval value set in [step 8](#).
8. Enter the interval in minutes in which throughput is measured and threshold notifications can occur. The valid range is 5 minutes to 70,560 minutes.

9. Click **Next**. A new screen displays for choosing ports for the alerts, as shown in Figure 51.

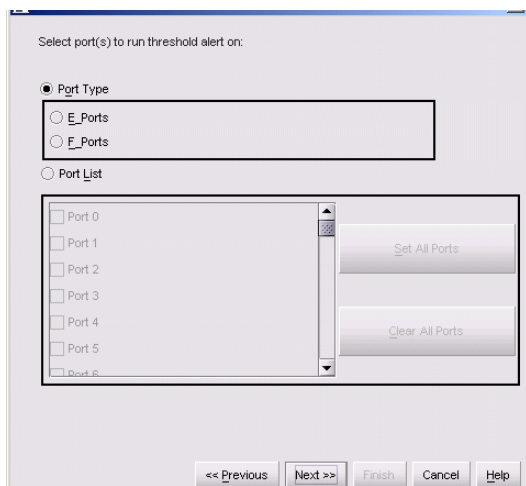


Figure 51 New Threshold Alerts dialog box - third screen

10. Click either **Port Type** or **Port List**.

- For **Port Type**, choosing either **E_Ports** or **F_Ports** will cause this alert to generate for all ports configured as E_Ports or F_Ports, respectively.
- For **Port List**, you can select individual ports when you click the check box by each port number or set all ports. Choosing **Set All Ports** places a check mark by each port number. Choosing **Clear All Ports** will clear the check marks by each port number.

11. Click **Next**. A final screen displays to provide a summary of your alert configuration, as shown in Figure 52.

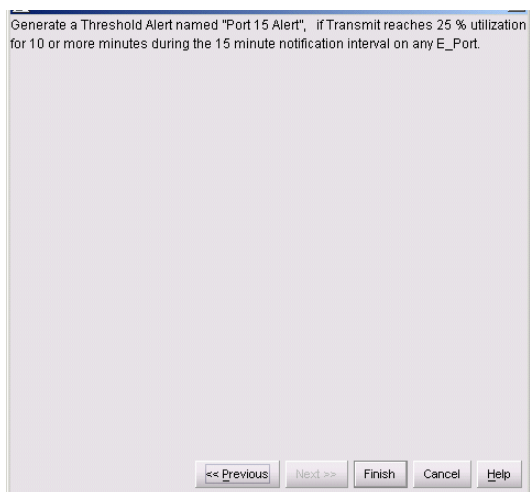


Figure 52 New Threshold Alerts dialog box - summary screen

12. Click **Finish**. The Configure Threshold Alerts dialog box displays listing the name, type, and state of the alert that you just configured.

13. At this point, the alert is not active. To activate the alert, select the alert information that displays in the **Configure Threshold Alerts** table and click **Activate**. The alert is activated, as shown in Figure 53.

Name	Type	State
90 alert	Receive And Transmit	Active
Port 15 Alert	Transmit	Inactive
test 2	Receive And Transmit	Inactive
test threshold	Receive And Transmit	Inactive

Figure 53 Configure Threshold Alerts dialog box - alert activated

Modifying alerts

Use the following steps to modify an existing threshold alert configuration.

1. At the Hardware view page, click **Configure > Threshold Alerts**. The Configure Threshold Alerts dialog box displays.
2. Select the alert that you want to modify when you click the alert information in the table. (If the alert is active, an error message displays prompting you to deactivate the alert.)
3. If the alert is active, click **Deactivate**, then select the alert information in the table again.
4. Click **Modify**. An initial Modify Threshold screen displays where you can change the threshold type.
5. Select a threshold type from the drop-down list.
6. Click **Next** when you are done. A Modify Threshold screen displays. You can use this screen to change the % utilization, cumulative minutes for the threshold to occur before notification, and the time interval for measuring throughput and for alert notification.
7. Make appropriate changes. Then, continue through the Modify Threshold screens, making changes as necessary, until the summary screen displays the alert configuration.
8. Perform either of the following steps:
 - If you need to change any parameters, click **Previous** or **Next** to display the desired Modify Threshold screen.
 - Click **Finish** when you are done.

Activating or deactivating alerts

Use the following steps to activate or deactivate existing threshold alerts. In the active state, notifications are generated for the alert. In the inactive state, notifications do not occur.

1. At the Hardware view page, click **Configure > Threshold Alerts**. The Configure Threshold Alerts dialog box displays.
The port's current state, inactive or active, is listed under the **State** column.
2. To change the state, select the alert by the alert information in the table.
3. If the alert is active, click **Deactivate** to change to the inactive state. If the alert is inactive, click **Activate** to change to the active state.

Deleting alerts

Use the following steps to delete existing threshold alerts.

1. At the Hardware view page, click **Configure > Threshold Alerts**. The Configure Threshold Alerts dialog box displays.
2. Select the alert that you want to delete by selecting the alert information in the table and clicking **Delete**. A message displays asking you to confirm the deletion.
3. Click **Yes**. The alert is removed from the dialog box.

Configuring open trunking

This option is only available if the optional Open Trunking feature is installed. Choosing this option opens the Configure Open Trunking dialog box. For details on enabling Open Trunking and configuring such parameters as congestion thresholds for ports, event notification options, and low BB_Credit threshold, see "[Open trunking](#)" on page 165.

Exporting the configuration report

Use this option to save an ASCII file of configuration data currently saved in director NV-RAM to your hard drive or a diskette. Use any desktop publishing application to import this ASCII file for viewing or printing.



NOTE: This file cannot be used to set configuration parameters through the Element Manager.

Data in the file includes:

- **Product identification**—Data from the Configure Identification dialog box.
- **Operating parameters**—Data from the Operating Parameters dialog box.
- **Port parameters**—Data from the Configure Ports dialog box.
- **SNMP parameters**—Data from the Configure SNMP dialog box.
- **Active zoning configuration**—This specifies the active zone and zone members, if set, and whether the default zone is enabled or disabled.

To export a configuration report:

1. Click **Configure > Export Configuration Report**. The Export Configuration Report dialog box displays, as shown in Figure 54.



- | | |
|---------------------|-------------------|
| 1 Details | 4 Home |
| 2 List | 5 Go up one level |
| 3 Create new folder | 6 Drive list |

Figure 54 Export Configuration Report dialog box

2. Select the folder where you want to save the file.
3. Type in a file name and extension in the **File name** field.
4. Click **Save**. The file saves to the specified folder as an ASCII text file.

Enabling Embedded Web Server

Use the following steps to enable EWS:

1. At the Hardware view page, click **Configure > Enable Web Server**. Choosing **Enable Web Server** automatically places a check mark in the check box.
2. Click **Enable Web Server** again to remove the check mark and disable the EWS interface. When disabled, remote users cannot access the interface.

For complete procedures on using EWS, refer to *HP StorageWorks Embedded Web Server user guide*.

Enabling Telnet

Use the following steps to enable Telnet:


1. At the Hardware view, click **Configure > Enable Telnet**. Choosing **Enable Telnet** automatically places a check mark in the check box.
2. Click **Enable Telnet** again to remove the check mark and disable Telnet access. When disabled, remote users cannot access the director through Telnet.

Enabling Alternate Control Prohibited

You can display Alternate Control Prohibited (ACP) in the Configure menu by selecting the checkbox to set the ACP on or off. When the ACP is checked, alternate control prohibited is on and alternate managers cannot change FICON switch connectivity parameters.

These parameters include all configuration changes including, but not limited to blocking ports, beaconing ports, clearing, LINs, CTP switch over and so on. The alternate managers include CLI, EWS, SNMP, but do not include the host via inband management.


The ACP setting is only controlled by the HAFM and cannot be changed by Host Programming. Select the option again to remove the check mark and disable Alternate Control Prohibited.


 **NOTE:** The Alternate Control Prohibited checkbox is only visible for switches that support ACP. Prior to sending the ACP setting to the switch, confirm the warning dialog box that displays that states you are about to disable alternate configuration control.

Backing up and restoring configuration data

You can back up the NV-RAM configuration, which includes all of the data you input through instructions in this chapter, using the **Backup and Restore Configuration** option. This option is available through the **Maintenance** menu. Selecting this option backs up the configuration data to a file on the HAFM appliance hard drive. The restore function writes this data back to NV-RAM on the switch. Using the restore function overwrites the existing configuration. For more information, see ["Backup and restore configuration"](#) on page 144.

In addition to the **Backup and Restore Configuration** option, the backup application automatically backs up configuration and other critical data from the HAFM appliance. As long as backup media remains in the CD-RW drive of the HAFM appliance, data is written to the backup media whenever the directory contents change or you reboot the HAFM appliance. For more information, see ["Backing up and restoring Element Manager data"](#) on page 47.

 **NOTE:** We do not recommend changing the default backup settings.

 **CAUTION:** To ensure trouble-free backups, it is imperative that you leave the backup media in the drive at all times. Removing the media during a backup or restore can corrupt the database on the media.

When data is being written to or read from the backup drive, the CD-RW drive write LED flashes. Make sure this LED is not flashing before you remove the media.

4 Using logs

This chapter describes the StorageWorks Director 2/64 and Director 2/140 logs. Access these logs from the Logs menu on the menu bar:

- [Using logs](#), page 125
- [Audit log](#), page 127
- [Event log](#), page 128
- [Hardware log](#), page 130
- [Link Incident log](#), page 132
- [Threshold Alert log](#), page 133
- [Open Trunking Log](#), page 133
- [Security log](#), page 134
- [Embedded Port log \(Advanced log\)](#), page 135
- [Switch Fabric log \(Advanced log\)](#), page 137

Using logs

The Audit, Event, Hardware, and Link Incident Logs store up to 1,000 entries each. The most recent entry appears at the top of the log. After 1,000 entries are stored, new entries overwrite the oldest entries.

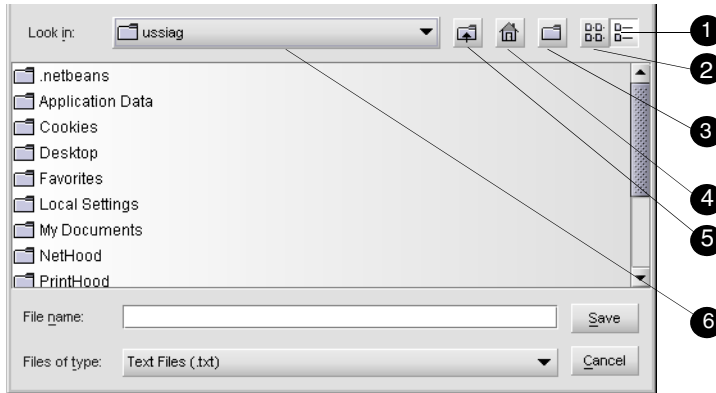
Button functions

Button function is the same for all logs:

- **Clear**—Clears all entries in the log for all users. A warning dialog box appears requesting confirmation that you want to clear all entries in the log.
- **Refresh**—Reads the current data and refreshes the screen with the new display.
- **Close**—Closes the log and displays the Director Element Manager window.
- **Export**—When you click **Export** on a log window, it displays the Save dialog box shown in [Figure 55](#) on page 126. Click the Home icon to return to the files in your home directory. The folders listed in the display area of the Save dialog box, after you click the Home icon, are those that are stored in your home directory. You can create a folder for your home directory and save the file there.

To save a log file in American Standard Code for Information Exchange (ASCII) format to a location on your system's hard drive or to a diskette, use the following steps. You can open this file in any desktop publisher for viewing or printing.

1. Click **Export** on the log window to display the Save dialog box. This dialog box contains the controls shown in [Figure 55](#).



- | | |
|---------------------|-------------------|
| 1 Details | 4 Home |
| 2 List | 5 Go up one level |
| 3 Create new folder | 6 Drive list |

Figure 55 Save dialog box—log windows

2. In the Save dialog box, select the folder where you want to save the file.
3. Type in a file name and extension in the **File name** field.
4. Click **Save**. The file saves to the specified folder as an ASCII text file.

Expanding columns

Expand columns in logs by placing the mouse pointer over the line separating column headings until a double arrow appears, then hold down the left mouse button and widen the column as necessary.

Sorting entries

Sort log entries in columns when you click a column heading. A down arrow in the header indicates sorting in descending order. An up arrow indicates sorting in ascending order. Click once to sort. Click again to reverse the sort.

Audit log

The Audit Log displays a history of all configuration changes applied to the director from any source such as HAFM, SNMP management stations, or host.

Date/Time	Action	Source	Identifier
2003/09/02 12:32:...	Operating Mode ch...	Application Interface	admin@172.18.3...
2003/09/02 12:30:...	Operating Mode ch...	Application Interface	admin@172.18.3...
2003/09/02 12:08:...	Operating Mode ch...	Application Interface	admin@172.18.3...
2003/09/02 12:06:...	Operating Mode ch...	Application Interface	admin@172.18.3...
2003/09/02 12:05:...	Operating Mode ch...	Application Interface	admin@172.18.3...
2003/09/02 12:02:...	Operating Mode ch...	Application Interface	admin@172.18.3...
2003/09/02 11:59:...	Operating Mode ch...	Application Interface	admin@172.18.3...
2003/09/02 11:58:...	New Feature Key L...	Application Interface	admin@172.18.3...

Figure 56 Audit log

Some actions, such as backing up configuration data and enabling automatic date/time synchronization, are performed only by the HAFM appliance without director interaction. These actions are indicated when HAFM displays in the **Source** column, as shown in Figure 56. If HAFM does not display, the time stamp is from the director.

- **Date/Time**—The date and time of the change on the director.
- **Action**—User action that caused the configuration change, such as offline status, port name change, or change of address.
- **Source**—Identifies the user making the change through the Director Element Manager and IP or DNS host name address of the remote user’s workstation.
 - Maintenance Port—Change was made by a user connected to the maintenance port.
 - HAFM application—Change was made by an Element Manager user.
 - SNMP—Change was made by a remote SNMP management station.
 - Fabric—Change was initiated by another director in the fabric that is not managed by this HAFM appliance.
 - Web server—Change was made by a user through the Embedded Web Server interface.
 - Fibre Channel Host—Change was made inband by a Fibre Channel host through the Open Systems or FICON management server.
 - Telnet—Change was made through a Telnet connection.

- **Identifier**—Identifies the user making the change according to the source:
 - Maintenance Port—No entry displays.
 - HAFM application—Includes user@address, where “user” is the Element Manager user name, and “address” is the network address of the workstation (remote user workstation or HAFM appliance).
 - SNMP—Contains the network address of the SNMP management station.
 - Fabric—No entry displays.
 - Web Server—The **Identifier** column contains user@address, where “user” is the web server user name and “address” is the network address of the web user.
 - Fibre Channel Host—No entry displays.
 - Telnet—Change was made through a Telnet connection.

Event log

The Event log provides a record of significant events that have occurred on the director, such as hardware failures, degraded operation, port problems, FRU failures, FRU removals and replacements, port problems, Fibre Channel link incidents, and HAFM appliance to director communication problems. The information is useful to maintenance personnel for fault isolation and repair verification.

Date/Ti...	Event	Description	Severity	FRU-Position	Event Data
2003/09/02...	411	Firmware fault occur...	WARNING	14	
2003/09/02...	81	Port set to invalid atta...	WARNING	14	
2003/09/02...	305	A cooling fan propelle...	WARNING	1	

Export...
Clear
Refresh
Close
Help

Figure 57 Event log

All detected firmware faults and hardware failures are sent to the HAFM appliance and recorded in the Event Log. The log provides a maximum of 1,000 log entries before it wraps and overwrites the oldest entries.

For detailed information on event data and problem resolution, refer to the *HP StorageWorks Director 2/64 service manual* for the Director 2/64 and the *HP StorageWorks Director 2/140 service manual* for the Director 2/140.

Each log entry includes the following:

- **Date/Time**—The date and time of the event on the director
- **Event**—Events are identified by a unique code. Event codes include:

Table 5 Event codes

Code	Event
000–199	System events
200–299	Power supply events
300–399	Fan module events
400–499	CTP card events
500–599	Port card events
600–699	SBAR card events
800–899	Thermal events

The following acronyms may display in this column for the port card:

- GLSL—G_Port, long wave, single-mode LC connector, 1 Gigabit
- GSML—G_Port, short wave, multi-mode, LC connector, 1 Gigabit
- GXXL—G_Port, mixed mode, LC connector, 1 Gigabit
- FPM—G_Port, small form factor pluggable (SFP) optics, FICON port module, 1 Gigabit
- UPM—G_Port, small form factor pluggable (SFP) optics, universal port module, 2 Gigabit
- GSF2—G_Port, small form factor pluggable (SFP) optics, universal port module, 2 Gigabit
- GLSR—G_Port, short wave, single-mode, MT-RJ connector, 1 Gigabit
- GXXR—G_Port, mixed mode, MT-RJ connector, 1 Gigabit
- GSMR—G_Port, short wave, multi-mode, MT-RJ connector, 1 Gigabit

The chassis (slot) position for a non-redundant FRU is 0. The chassis positions for redundant FRUs are 0, 1, and 2. The chassis positions for port cards are 0 through 35, and slot 32 is unavailable.

- **Description**—A short description of the event
- **Severity**—There are four classifications of severity that identify the importance of the event.
 - 0=Informational
 - 2=Warning
 - 3=Fatal
 - 4=Fatal, not operational

- **FRU Position**—An acronym representing the FRU type, followed by a number representing the FRU chassis position. FRU acronyms are:
 - **CTP**—CTP card
 - **FAN**—fan module
 - **PWR**—power supply

The chassis (slot) position for a non-redundant FRU is 0. The chassis positions for redundant FRUs are 0, 1, and 2. The chassis positions for port cards are 0 through 35, and slot 32 is unavailable.

- **Event Data**—Up to 32 bytes of supplementary information for the event in hexadecimal format. For detailed information on event data and problem resolution, refer to the event code tables appendix in the *HP StorageWorks Director 2/64 service manual* for the Director 2/64 and the *HP StorageWorks Director 2/140 service manual* for the Director 2/140.

Hardware log

The Hardware log displays information on FRUs inserted and removed from the director.

Date/Time	FRU	Position	Action	Part Number	Serial Number
2004/04/26 1...	Serial Cross...	1	Inserted	254133-001	21101294
2004/04/26 1...	Serial Cross...	1	Removed	254133-001	21101294
2004/04/26 1...	Control Proc...	1	Inserted	254136-001	81391521
2004/04/26 1...	Control Proc...	1	Removed	254136-001	81391521
2004/04/26 1...	G Port Modul...	8	Inserted	292006-001	82072689
2004/04/26 1...	G Port Modul...	8	Removed	292006-001	82072689

Figure 58 Hardware log

Each log entry includes the following:

- **Date/Time**—Date and time of the insertion or removal of the FRU
- **FRU**—The name of the inserted or removed FRU

Table 6 FRU names

FRU Code	FRU Name
FAN	Fan module
PWR	Power supply module
CTP	Control processor
SBAR	SBAR card
BKPLNE	Backplane

The following acronyms may display in this column for the port card:

- GLSL—G_Port, long wave, single mode LC connector, 1 Gigabit
- GSML—G_Port, short wave, multimode, LC connector, 1 Gigabit
- GXXL—G_Port, mixed mode, LC connector, 1 Gigabit
- FPM—G_Port, small form factor pluggable (SFP) optics, FICON port module, 1 Gigabit
- UPM—G_Port, small form factor pluggable (SFP) optics, universal port module, 2 Gigabit
- GSF2—G_Port, small form factor pluggable (SFP) optics, universal port module, 2 Gigabit
- GLSR—G_Port, short wave, single mode, MT-RJ connector, 1 Gigabit
- GXXR—G_Port, mixed mode, MT-RJ connector, 1 Gigabit
- GSMR—G_Port, short wave, multimode, MT-RJ connector, 1 Gigabit
- **Position**—Slot position in the chassis relative to identical components installed
- **Action**—Inserted or removed
- **Part Number**—Part number of the component
- **Serial Number**—Serial number of the component

Link Incident log

The Link Incident Log displays the 1,000 most recent link incidents with the date the incident occurred, the time it occurred, and the port on which the incident took place. The information is useful to maintenance personnel for isolating port problems [particularly expansion port (E_Port) segmentation problems] and repair verification.

Date/Time	port	Link Incident
2003/09/02 17:01:54	0	Bit Error Threshold Exceeded
2003/09/02 16:54:40	13	Implicit Incident
2003/09/02 15:56:39	12	NOS Received

Export...

Clear

Refresh

Close

Help

Figure 59 Link Incident Log

Each log entry contains:

- **Date/Time**—The date and time of the incident.
- **Port**—The number of the port on which the incident occurred.
- **Link Incident**—A short description of the incident. The following events may cause a link incident to be written to the log.
 - Implicit incident—The attached node detects a condition that may cause problems on the link.
 - Bit-error threshold exceeded—The number of code violation errors has exceeded threshold.
 - Loss-of-signal or loss-of-synchronization. This occurs if a cable is unplugged from an attached node. Loss-of-synchronization condition has persisted for longer than the resource allocation time out value (R_A_TOV).
 - Not-operational (NOS) primitive sequence received—A NOS was recognized.
 - Primitive sequence timeout. Link reset protocol timeout occurred. Timeout occurred for an appropriate response while in NOS receive state and after NOS is no longer recognized.
 - Invalid primitive sequence received for the current link state—Either a link reset or a link reset response primitive sequence was recognized while waiting for the offline sequence.

For corrective actions in response to these link incident messages, refer to the diagnostics chapter in the *HP StorageWorks Director 2/64 service manual* for the Director 2/64 and the *HP StorageWorks Director 2/140 service manual* for the Director 2/140.

Threshold Alert log

This log provides details of threshold alert notifications. Besides the date and time that the alert occurred, the log also displays details about the alert as configured through the **Configure Threshold Alerts** option under the **Configure** menu on the menu bar.

Date/Time	Name	Port	Type	Utilization %	Interval
2003/09/03 1...	Port 1 50%	1	Receive And...	50	5
2003/09/03 1...	Testing	7	Receive And...	50	5
2003/09/03 1...	75%	7	Receive And...	75	5
2003/09/03 1...	Testing	3	Receive And...	50	5
2003/09/03 1...	Testing	5	Receive And...	50	5
2003/09/03 1...	75%	3	Receive And...	75	5
2003/09/03 1...	75%	5	Receive And...	75	5
2003/09/03 1...	Testing	1	Receive And...	50	5
2003/09/03 1...	75%	1	Receive And...	75	5
2003/09/03 1...	Port 5 & 7 70%	5	Receive And...	70	5
2003/09/03 1...	Port 5 & 7 70%	7	Receive And...	70	5
2003/09/03 1...	Port 3 75%	3	Receive And...	75	5
2003/09/03 1...	Port 1 50%	1	Receive And...	50	5
2003/09/03 1...	Testing	7	Receive And...	50	5
2003/09/03 1...	75%	7	Receive And...	75	5
2003/09/03 1...	Testing	3	Receive And...	50	5
2003/09/03 1...	Testing	5	Receive And...	50	5
2003/09/03 1...	75%	3	Receive And...	75	5
2003/09/03 1...	75%	5	Receive And...	75	5
2003/09/03 1...	Testing	1	Receive And...	50	5
2003/09/03 1...	75%	1	Receive And...	75	5
2003/09/03 1...	Port 5 & 7 70%	5	Receive And...	70	5
2003/09/03 1...	Port 5 & 7 70%	7	Receive And...	70	5
2003/09/03 1...	Port 3 75%	3	Receive And...	75	5

Figure 60 Threshold Alert log

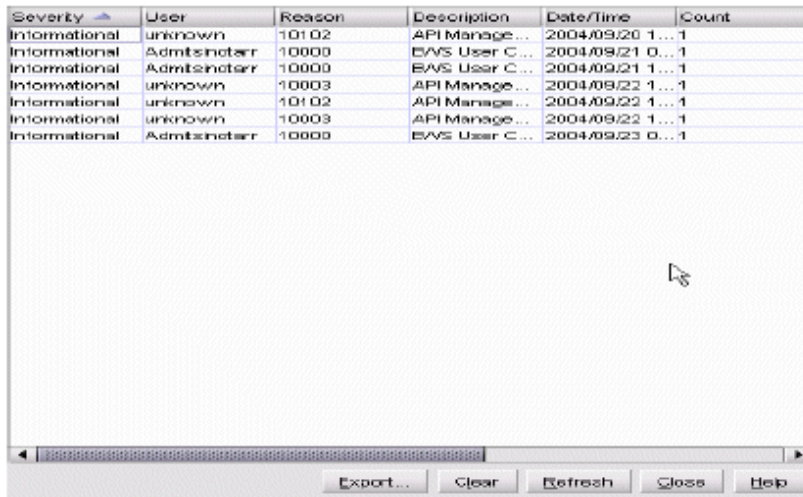
- **Date/Time**—Date and time stamp for when the alert occurred.
- **Name**—Name for the alert as configured through the Configure Threshold Alerts dialog box.
- **Port**—Port number where the alert occurred.
- **Type**—The type of alert: transmit (Tx) or receive (Rx).
- **Utilization %**—Percent usage of traffic capacity. This is the percent of the port’s throughput capacity achieved by the measured throughput. This setting constitutes the threshold value and is configured through the Configure Threshold Alerts dialog box. For example, a value of 25 means that threshold occurs when throughput reaches 25 percent of the port’s capacity.
- **Alert Time**—The time that the utilization % must exist before an alert is generated. This is set through the Configure Threshold Alerts dialog box.
- **Interval**—The time interval during which the throughput is measured and an alert can generate. This is set through the Configure Threshold Alerts dialog box.

Open Trunking Log

This log displays only if the optional Open Trunking feature is installed. For details, see “[Open Trunking Log](#)” on page 169.

Security log

The Security log includes information about security events, as shown in [Figure 61](#).



The screenshot shows a window titled 'Security log' with a table of events. The table has six columns: Severity, User, Reason, Description, Date/Time, and Count. The data is as follows:

Severity	User	Reason	Description	Date/Time	Count
Informational	unknown	10102	API Manage...	2004/09/20 1...	1
Informational	Adminstrator	10000	EWS User C...	2004/09/21 0...	1
Informational	Adminstrator	10000	EWS User C...	2004/09/21 1...	1
Informational	unknown	10003	API Manage...	2004/09/22 1...	1
Informational	unknown	10102	API Manage...	2004/09/22 1...	1
Informational	unknown	10003	API Manage...	2004/09/22 1...	1
Informational	Adminstrator	10000	EWS User C...	2004/09/23 0...	1

Below the table is a search bar and a set of buttons: Export..., Clear, Refresh, Close, and Help.

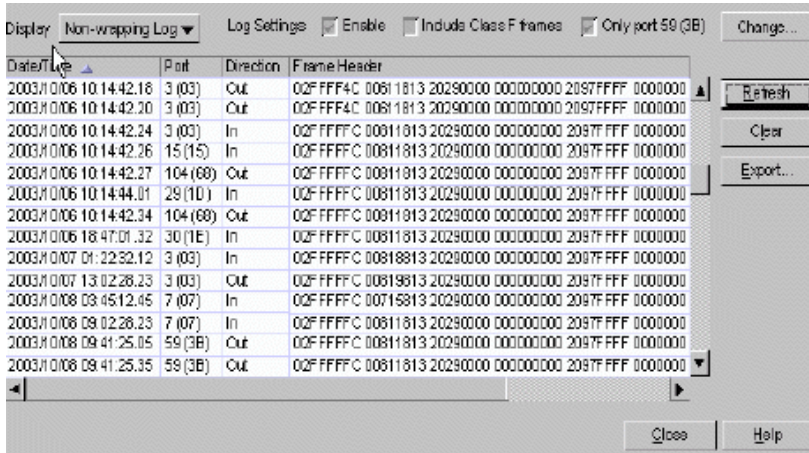
Figure 61 Security log

The Security log displays the following information:

- **Severity**—The severity level of the event, informational, warning, and fatal.
- **User**—The user associated with the event.
- **Reason**—The reason code for caused the failure.
- **Description**—The security event category and includes the description that lists more details of the event and the IP address of the product.
- **Date and Time**—The date and time that the event occurred. The format is *yyyy/mm/dd hh:mm:ss:tt*. The last two characters (hundredth of seconds) are needed due to possible higher frequency rate of some of the advanced logs.
- **Count**—The number of times that the same event occurs.
- **Category**—The category.
- **IP**—The IP address.
- **Role**—The role of the user.
- **Interface**—The interface.

Embedded Port log (Advanced log)

This log provides a detailed history log of all traffic passing through the embedded port. The Embedded Port (EP) of the Switch is a single physical FC port within the hardware architecture that is used to communicate FC frames between devices attached to the external ports and the embedded firmware's FC services software, based on the use of well-known Fibre Channel addresses. This is similar to the function of the Control Unit Port (CUP) in FICON architecture. The CUP is implemented via the EP for FICON traffic. The Embedded Port Log will log all FC frame traffic directed to the switch (EP), including discards, frames not routed, and traffic designated for the EP (inband traffic), as shown in [Figure 62](#).



Date/Time	Port	Direction	Frame Header
2003/10/06 10:14:42.18	3 (03)	Out	02F FFF4C 00811813 20290000 00000000 2097FFF 0000000
2003/10/06 10:14:42.20	3 (03)	Out	02F FFF4C 00811813 20290000 00000000 2097FFF 0000000
2003/10/06 10:14:42.24	3 (03)	In	02F FFFFC 00811813 20290000 00000000 2097FFF 0000000
2003/10/06 10:14:42.26	15 (15)	In	02F FFFFC 00811813 20290000 00000000 2097FFF 0000000
2003/10/06 10:14:42.27	104 (68)	Out	02F FFFFC 00811813 20290000 00000000 2097FFF 0000000
2003/10/06 10:14:44.01	29 (10)	In	02F FFFFC 00811813 20290000 00000000 2097FFF 0000000
2003/10/06 10:14:42.34	104 (68)	Out	02F FFFFC 00811813 20290000 00000000 2097FFF 0000000
2003/10/06 18:47:01.32	30 (1E)	In	02F FFFFC 00811813 20290000 00000000 2097FFF 0000000
2003/10/07 01:22:52.12	3 (03)	In	02F FFFFC 00818813 20290000 00000000 2097FFF 0000000
2003/10/07 13:02:28.23	3 (03)	Out	02F FFFFC 00819813 20290000 00000000 2097FFF 0000000
2003/10/08 03:45:12.45	7 (07)	In	02F FFFFC 00715813 20290000 00000000 2097FFF 0000000
2003/10/08 08:02:28.23	7 (07)	In	02F FFFFC 00811813 20290000 00000000 2097FFF 0000000
2003/10/08 09:41:25.05	59 (3B)	Out	02F FFFFC 00811813 20290000 00000000 2097FFF 0000000
2003/10/08 09:41:25.35	59 (3B)	Out	02F FFFFC 00811813 20290000 00000000 2097FFF 0000000

Figure 62 Embedded Port log (FICON style display mode)

- **Non-wrapping Log or Wrapping Log**—From the submenu, select Non-wrapping log or Wrapping log, Wrapping log is the default.
- **Log Settings**—Displays the current settings of the log options configured on the Switch. These settings affect how log data is captured and stored on the Switch, not just what is displayed in the dialog box. For example, if the Include Class F Frames is turned off or unchecked, Class F frames are not captured or stored in the log on the Switch and are not accessible from this log. To change these options, click **Change**. For information, Change button-136
- **Date and Time**—The date and time that the event occurred. The format is *yyyy/mm/dd hh:mm:ss:tt*. The last two characters (hundredth of seconds) are needed due to possible higher frequency rate of some of the advanced logs.
- **Port**—The decimal receive port number on the local Switch associated with the flow that was rerouted. When FICON style is on, the hexadecimal equivalent of the port number displays in parentheses. When FICON style is off, only the decimal value is shown and there is no value in the parenthesis.
- **Direction**—**In** or **Out** indicates the direction of the frame in reference to the embedded port and is related to the port number. For example, if **In** displays, then the frame is coming into the embedded port from the port number specified in the **Port** box.

- **Frame Header**—The Fibre Channel Frame Header string. This header is not interpreted by the Element Manager. The table cell contents can be copied into a third party application for interpretation.
- **Length**— Length of the payload, byte counter, decimal display format. Since the payload can be longer than the maximum 32 bytes retained by the log, this value displays how many bytes are actually in the frame.
- **Payload**—The payload portion of the data box.
- **SOF**—The string that contains the Start of Frame code abbreviation. Place the cursor over a cell in this column to display descriptions of the abbreviation.
- **EOF**—The string that contains the End of Frame code abbreviation. Place the cursor over a cell in this column to display descriptions of the abbreviation.

Change button

If Administrator or Maintenance user rights are set to access the button, you can display the Embedded Port Log Settings Dialog box. If you do not have access to this button, an error dialog box appears.

This dialog box log provides a detailed history log of all traffic passing through the embedded port, as shown in [Figure 63](#).

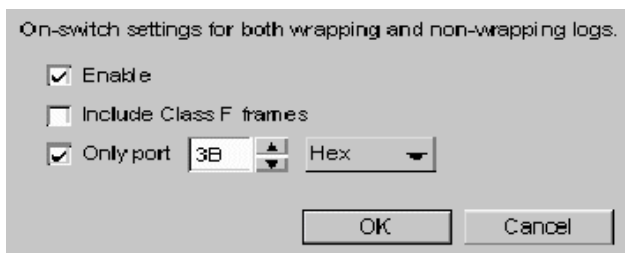



Figure 63 Log Settings dialog box

 **NOTE:** If not in FICON style mode, the Hex/Dialog option is not displayed and entries are only made in decimal.

- **Enable**—Turns logging on (default=checked) or off (unchecked) for the currently displayed log (either wrapping or. Implemented on the switch as trace filter set to no ports (TRACE_NO_PORTS).
- **Include Class F Frame**—When this option is checked, which is the default, all frames received are stored in the log, unless port filtering logs only one port. When unchecked, no Class F frames are logged.

- **Only Port**—When this option is unchecked, which is the default, frames from all ports are logged. F frames depend on the **Include Class F Frame** option. When checked, the port entry box is enabled, and the port number to be logged can be entered. When in FICON Style mode-, port numbers can be entered into this box in either in hex or decimal using **Hex/Decimal**. The spin button limits port number entries to valid ranges, including the exclusion of unavailable port numbers. After selecting **OK** from this port selection dialog, the selected port number is displayed on the main log dialog next to the **Only port** check box (such as, **Only port 59**, or **Only port 59 (3B)** if in FICON style mode). Only frames from or to the selected port are retained in the switch's log after that point.

Switch Fabric log (Advanced log)

The Switch Fabric log includes switch fabric information as shown in [Figure 64](#).

Date/Time	Description	Event Data	Ports (RSCN only)
2003/10/06 10:14:42.18	Start Build Fabric	Switch power-on (Port=32)	
2003/10/06 10:14:42.20	Invalid Attachment Rec...	Port=15, Reason=xxx	
2003/10/06 10:14:42.24	FabricInit Completed		
2003/10/06 10:14:42.26	Paths Operational		
2003/10/06 10:14:42.27	Fabric Operational		
2003/10/06 10:14:44.01	E_Port entered FSPF F	Port=48	
2003/10/06 10:14:42.34	Start Zone Merge	E_Port entered FSPF Full state	
2003/10/06 10:18:01.32	Zone Merge Failure	Port=17, Response=39290	
2003/10/07 01:22:30.12	Port RSCN	Invalid xxx, Port offline	2,3,5,7,18,25,36,37,38,
2003/10/07 14:02:52.37	Port RSCN	Invalid xxx, Port online	7,8,9,10,11,12,32,33,34
2003/10/07 14:02:52.37	Invalid Attachment Rec	Port=8, Reason=yyy	
2003/10/07 14:02:52.37	FabricInit Completed		
2003/10/06 09:41:25.05	Domain ID Change	New DID=5, Preferred Do	
2003/10/06 09:41:25.12	FabricInit Completed		

Figure 64 Switch Fabric log

This log displays the following information about switches in a fabric:

- **Non-wrapping Log or Wrapping Log**—From the submenu, select **Non-wrapping log** or **Wrapping log**. **Wrapping log** is the default.
- **Date and Time**—The date and time that the event occurred. The format is *yyyy/mm/dd hh:mm:ss:tt*. The last two characters (hundredth of seconds) are needed due to possible higher frequency rate of some of the advanced logs.
- **Description**—The description string for the event type. The string content is displayed directly as stored in the log.
- **Event Data**—This string contains details of the event, and is variable depending on the event logged. This is provided directly by the log content, and is displayed here exactly as received.
- **Ports (RSCN only)**—For Port RSCN events only, a list of affected ports is displayed in this column. This is interpreted from port bitmap data stored in the log, and only the ports with a bit value of 1 are listed. If there are many bits set in a large switch, the contents of this box can be very long.

5 Using maintenance features

This chapter describes how to use the options that display under the **Maintenance** menu on the menu bar along the top of the Element Manager window. The following options are described:

- [Port diagnostics](#), page 140
- [Swap ports \(FICON management style\)](#), page 140
- [Collect maintenance data](#), page 141
- [Execute an IPL](#), page 141
- [Set online state](#), page 142
- [Manage firmware versions](#), page 143
- [Enable e-mail notification](#), page 143
- [Enable call-home notification](#), page 144
- [Backup and restore configuration](#), page 144
- [Reset configuration](#), page 146

Port diagnostics

The **Port Diagnostics** option enables you to run internal and external loopback tests on any port or all ports on a port card. At the start of the loopback test, the port or port card can be online, offline, blocked, or unblocked

- **Internal loopback test** —An internal loopback test checks port circuitry, but does not check fiber-optic components of a port transceiver. The test is performed with a device attached to the port, but the test momentarily blocks the port and is disruptive to the attached device.
An optical transceiver (SFP or XFP) must be installed in the port during the test. A device can remain connected during the test.
- **External loopback test** —An external loopback test checks port circuitry, including fiber-optic components of a port transceiver. To perform the test, the attached device must be acquiesced and disconnected from the port, and a multimode or singlemode loopback plug must be inserted in the port receptacle.

To use this option, follow the detailed steps in the *HP StorageWorks Director 2/64 service manual* for the Director 2/64 and the *HP StorageWorks Director 2/140 service manual* for the Director 2/140.

Swap ports (FICON management style)

This procedure applies only to a director that is using FICON Management Style.

Select **Swap Ports** to display the Swap Ports dialog box. Use this dialog box to swap one port address for another. For example, if the current address for port 0 is currently 04 and the address for port 1 is currently 05, you can swap so that the address for port 0 has address 05 and port 1 has address 04.

To swap ports, use the following steps:

1. Select **Swap Ports** from the **Maintenance** menu on the menu bar. The Swap Ports dialog box appears, as shown in [Figure 65](#).

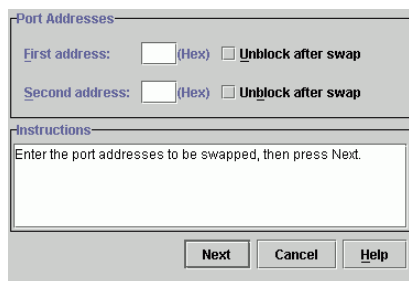


Figure 65 Swap Ports dialog box

2. Enter the first address (in hexadecimal format).
3. If you want to unblock the port, select **Unblock after swap** option. Note that ports are automatically blocked during the swap process.
4. Enter the second address (in hexadecimal format).


5. If you want to unblock the port, select **Unblock after swap** option.
6. Click **Next** to continue.
7. Follow the on-screen instructions and click **Next** to continue through to the next screen.
8. If you are finished configuring the director, back up the configuration data. For more information, see "[Backup and restore configuration](#)" on page 144.

Notes

- Make sure that the system administrator varies devices offline that are attached to the ports whose addresses you are going to swap.
- Ports that you are going to swap are blocked during this procedure, as swapping ports is disruptive to port operation.

Collect maintenance data


The Data Collection option enables you to collect maintenance data that can help support personnel diagnose system problems. Save the maintenance data as a zip file on a backup disk (or other medium with the appropriate capacity), and forward it to technical support personnel.

 **NOTE:** If the Full Volatility feature is enabled through the director's maintenance port, a memory dump file is not included with the data collection.

To use this option, follow the detailed steps in the *HP StorageWorks Director 2/64 service manual* for the Director 2/64 and the *HP StorageWorks Director 2/140 service manual* for the Director 2/140.

Execute an IPL

△ **CAUTION:** The Ethernet connection between the HAFM appliance and director is interrupted momentarily during an IPL.

 **NOTE:** An initial program load (IPL) is not intended for ordinary or casual use and should only be performed if the active CTP card is suspected to be faulty. This operation resets the active CTP card (an IML resets both CTP cards). Do not use this option unless directed by your support representative or if you need to reset a failed CTP card.

If it is necessary for you to execute an IPL on the director, use the following steps:

1. Select **IPL** from the **Configure** menu on the menu bar. The IPL Confirmation dialog box appears, as shown in [Figure 66](#).

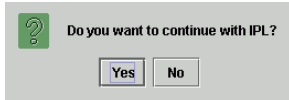


Figure 66 IPL Confirmation dialog box

2. Click **Yes**.

Choosing **IPL** from the **Maintenance** menu causes Ethernet connection between the director and HAFM appliance to drop momentarily. The following occurs in the Element Manager window:

- As the network connection drops, the Director **Status** table on the Hardware View turns yellow.
- The **Status** field in the table displays `No Link`, and the **State** field displays the reason for no link.
- A gray square appears in the status bar. See [Table 2](#) on page 43 for an explanation of this status bar display.
- The FRUs in the illustration in the Hardware View do not display. They display again as the connection is reestablished.

For details on functions performed by an IPL, refer to the *HP StorageWorks Director 2/64 service manual* for the Director 2/64 and the *HP StorageWorks Director 2/140 service manual* for the Director 2/140.

Set online state

Use the procedure in this section to display the current director operating state (offline or online) and change the state as required. The director can have one of the following operational states:

- **Online**—When the director is in the online state, all of the unblocked ports are allowed to log in to the fabric and to begin communicating. Devices can connect to the director and communicate with another device if:
 - The port is not blocked.
 - The default zone is enabled or both devices are in the same zone.
- **Offline**—When the director is in the offline state, all the installed ports are offline. The ports transmit an OLS (offline sequence), and they cannot accept a login for connection from an attached device. All ports in the director, including E_Ports, are placed offline regardless of whether they were blocked or unblocked and the director is removed from a multiswitch fabric.

△ **CAUTION:** Before setting the director offline, warn administrators and users currently operating devices that are attached to the director that it is going offline and that there will be a disruption of communications. Make sure administrators of devices attached to ports quiesce Fibre Channel traffic through the director.

To set the director online or offline (depending on current state), right-click the director in the Hardware View and select **Set Online State** from the menu, or use the following steps:

1. Select **Set Online State** from the **Maintenance** menu on the menu bar.
2. Click **Set Offline** or **Set Online**, depending on the operating state you want to set.
3. When a warning box appears requesting you to confirm the offline or online state, click **OK**.


As the director goes offline, **OFFLINE** appears in the **State** field of the **Director Status** table in the Hardware View. LED indicators on all ports with attached devices stay green, but the director is sending offline sequences (OLS) to these devices.

Manage firmware versions

Firmware refers to the internal operating code for the director. You can maintain up to eight firmware versions on the HAFM appliance for downloading to a director. To use the **Firmware Library** option to manage firmware versions, follow the steps in the *HP StorageWorks Director 2/64 service manual* for the Director 2/64 and the *HP StorageWorks Director 2/140 service manual* for the Director 2/140.

Enable e-mail notification

E-mail addresses and the simple mail transfer protocol (SMTP) server address for e-mail notification of director events must be configured through the HAFM application. Refer to the *HP StorageWorks HA-Fabric Manager user guide* for instructions on configuring e-mail.

 **NOTE:** E-mail recipients are configured in the HAFM application through the Configure E-Mail dialog box. A valid SMTP address is configured in this dialog box.

Use the Enable E-Mail Notification function on the Element Manager to enable e-mail notification for events that occur on a selected director. The default state is disabled.

To enable e-mail notification, use the following steps:

1. Select **Maintenance > Enable E-Mail Notification** from the menu bar.
2. To enable e-mail notification, select the option to add a check mark to the check box.
3. To disable e-mail notification, select the option to remove the check mark from the check box.

Enable call-home notification

The call-home feature enables the HAFM appliance to automatically contact a support center to report system problems. The support center server accepts calls from the HAFM appliance, logs reported events, and notifies one or more support center representatives.

Use the Enable Call Home Notification function on the Element Manager to enable call-home notification for events that occur on the selected director. The default state is disabled.

Notes


- You must enable call-home event notification through the StorageWorks HAFM application **Maintenance** menu before enabling this function through the Element Manager for individual directors. A choice of two call-home features is provided when HAFM is installed.
- In legacy HP environments, call-home notification for directors and switches requires installation of Proactive Service software. This service is offered at no additional charge for subsystems covered under an on-site warranty or on-site storage hardware support contract. To register or order Proactive Services software, contact your HP customer service representative.
- In classic HP environments, configure telephone numbers and other information for the call-home feature through the Windows dial-up networking application. To enable call-home notification for a director, see *HP StorageWorks HA-Fabric Manager Application installation guide*.

A check mark appears next to the menu option to indicate that call-home notification is enabled.

Backup and restore configuration

Select this option to save the product configuration stored on the director to the HAFM appliance hard disk, or to restore the product configuration from the HAFM appliance. Only a single copy of the configuration is kept on the HAFM appliance.

The purpose of the backup is primarily for single-CTP systems, such as the director, where a backup is needed in order to restore a replacement CTP card. You can also use this feature for a special purpose configuration or for temporary testing of a configuration. You cannot modify the location and file name of the saved configuration.

 **NOTE:** You can only restore the configuration to a director with the same IP address.

Backup procedure

Use the following procedure to backup your product configuration:

1. Select **Backup and Restore Configuration** from the **Maintenance** menu on the menu bar. The Backup and Restore Configuration dialog box appears, as shown in [Figure 67](#).

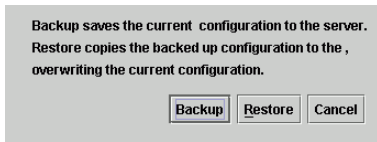


Figure 67 Backup and Restore Configuration dialog box

The Backup and Restore Configuration dialog box consists of a short description of the features performed when you select **Backup** or **Restore**.

2. Click **Backup** to save the current director configuration to the HAFM appliance. The following is a list of configurations that are backed up to the HAFM appliance:
 - Identification data (director name, description, and location).
 - Port configuration data (port names, blocked states, and extended distance settings).
 - Operating parameters [BB_Credit, E_D_TOV, R_A_TOV, director priority, preferred domain ID, rerouting delay, domain RSCNs, and director speed (Director 2/64 only)].
 - SNMP configuration (trap recipients, community names, and write authorizations).
 - Zoning configuration (active zone set and default zone state).

A backup is immediately attempted when you click **Backup** on this dialog box. A dialog box appears to confirm that the backup to the HAFM appliance is complete. If the backup fails, a dialog box appears to inform you that the backup to the HAFM appliance failed.

Restore procedure

Use the following procedure to restore your product configuration:

1. Set the director to offline before performing the restore function. If you click **Restore** and the director is online, a message dialog appears requesting that you turn the director offline. No action takes place when you close the dialog box. For instructions on setting the director offline or online, see "[Set online state](#)" on page 142.
2. Click **Restore** on the Backup and Restore Configuration dialog box to copy the backed up configuration to the nonvolatile random access memory (NV-RAM) on the director.

If the director is already offline and you click **Restore**, a confirmation dialog box appears indicating that the restore will overwrite any existing configurations already on the director and it displays the date of the restored backup.

NOTE: The restore operation initiates an IPL.

The **Export Configuration Report** function accessed through the **Configure** menu on the menu bar is an ASCII file of the backup performed in this section.

Reset configuration


This feature is used to reset all configuration data for the director to factory default values. You must have maintenance authorization rights to access this feature.

The Internet protocol (IP) address will reset to the factory default value during this procedure. You may not recover the Ethernet connection between the director and HAFM appliance if you have changed the director's IP addressing from that default value. In this case you must reenter LAN addressing, such as IP and gateway addresses, through a terminal attached to the maintenance port.

Before using the reset configuration option, record the director's current IP address, which displays below the icon in the HAFM application's Product View when the view's **Display Options** are set to **Network Address**. You can also find the current IP address through the Embedded Web Server interface.


After resetting the configuration, reset LAN addressing to the desired values through the maintenance port or the Embedded Web Server interface.

If you have enabled the Full Volatility feature through the director's maintenance port, this feature will disable when the configuration is reset.


 **NOTE:** Use of the maintenance port is not covered in this manual. For procedures, refer to the *HP StorageWorks Director 2/64 service manual* for the Director 2/64 and the *HP StorageWorks Director 2/140 service manual* for the Director 2/140.

Use the following steps to reset the configuration parameters on the director to the default values.

1. Select **Reset Configuration** from the **Maintenance** menu. The following warning appears:

 **WARNING!** This operation will reset all director configuration data and nonvolatile settings to factory default values. The director must be offline to continue.

2. Set the director offline. For instructions, see "[Set online state](#)" on page 142.
3. To continue the reset operation, click **Reset** on the Reset Configuration dialog box. If you want to cancel the operation, click **Cancel**.

 **NOTE:** If you have enabled features that add additional port function since the director was shipped from the factory, these features will be disabled (factory default) when the configuration is reset. Only those ports that were enabled at the factory will function. You will have to enable the additional port function features again through the **Configure Feature Key** dialog box.

Factory-default values may vary, depending on the firmware release installed in your director. For a list of values, refer to the *HP StorageWorks Director 2/64 service manual* for the Director 2/64 and the *HP StorageWorks Director 2/140 service manual* for the Director 2/140.

Table 7 Data default values

Configuration	Description	Default
Identification	Director Name	NULL string
	Director Description	"Fibre Channel Director"
	Director Contact	"End User Contact (please configure)"
	Director Location	"End User Contact (please configure)"
Ports	Port Names	NULL strings
	Port Blocked States	Unblocked
	Extended Distance (10–100 km)	Disabled
	RX BB Credit	Disabled
	LIN Alerts	Disabled
	Port Address	Port number plus 4
Director Addressing	IP Address	10, mac[3], mac[4], mac[5] converted to word32 MAC addresses are set in hexadecimal; IP addresses in decimal. A MAC address of 08 00 88 20 00 57 will be reset to an IP address of 10.32.0.87.
	Subnet Mask	255.0.0.0
	Gateway Address	0.0.0.0
	MAC Address	PROM value
Operating Parameters	Preferred Domain ID	1
	Buffer-to-Buffer Credit	16
	R_A_TOV	10 seconds (100 tenths)
	E_D_TOV	2 seconds (20 tenths)
	Director Priority	254
	Insistent	Disabled
	Rerouting Delay	Enabled
	Domain RSCNs	Disabled
	Suppress Zoning RSCNs	Disabled

Table 7 Data default values (continued)

Configuration	Description	Default
SNMP	SNMP Communities	"public"—5 NULL strings
	SNMP Write Authorizations	Read only per community
	Trap Recipient IP Addressees	0 for each
	UDP Port	162
	SNMP Authorization Trap State	5
Zoning	Number of Zone Members	0
	Number of Zones	0
	Number of Zone Sets	0
	Zone Names	None
	Zone Sets Names	None
	Zone Members	None
	Default Zone State	Disabled
	Active Zone Set State	Disabled
	Active Zone Set Name	NULL string

6 Optional features

This chapter provides detailed information on using, administering, and configuring optional HAFM's features through HAFM applications. There are two types of features covered in this chapter:

- Keyed features, requiring feature keys to be purchased and enabled through the Configure Feature Key dialog box in the product's Element Manager.
- Features not requiring feature keys themselves, but requiring that specific keyed features be enabled before they can be accessed through the HAFM or Element Manager.

The following sections are covered in this chapter:

- [Preferred Path](#), page 150
- [FICON management server](#), page 156
- [Open systems management server](#), page 158
- [SANtegrity features](#), page 159
- [Open trunking](#), page 165

Preferred Path

The Preferred Path feature enables you to influence the route of data traffic when traversing more than one Switch in a fabric. If more than one ISL connects switches in your SAN, this feature will be useful for specifying an ISL preference for a particular flow. The data path consists of the source port of the Switch or Director being configured, the exit port of that Switch or Director, and the domain ID of the destination Switch or Director. Each Switch or Director must be configured for its part of the desired path in order to achieve optimal performance. You may need to configure Preferred Paths for all Switches or Directors along the desired path for proper multi-hop Preferred Path operation.

Configuring a preferred path

The Preferred Path feature enables you to influence the route of data traffic when traversing multiple switches or directors in a fabric. If more than one ISL connects switches in your SAN, this feature will be useful for specifying an ISL preference for a particular flow. The data path consists of the following:

- Source port of the switch or director being configured
- Exit port of that switch or director
- Domain ID of the destination switch or director.

Each switch or director must be configured for its part of the desired path in order to achieve optimal performance. You may need to configure Preferred Paths for all switches or directors along the desired path for proper multi-hop Preferred Path operation. The following is an example of the procedure to use.

Adding a preferred path

To add a new preferred path, use the following steps:

-
- △ **CAUTION:** Activation of a new Preferred Path will cause a reroute to occur if the Preferred Path is different from the current path. In congested environments, with traffic on the current path, a reroute can cause an out of order frame (OOOF) at the destination device.
- Reroutes are a natural activity in any Fibre Channel fabric when the network is modified. For example, reroutes occur when ISLs are added or lost or when new switches are added to the fabric. Fibre Channel devices are designed to handle errors like OOOFs, but some send error messages when they occur.
 - In FICON environments, an IFCC error can result from an OOOF. To avoid these error messages, devices should be varied offline before a Preferred Path is activated, and returned to online status after the activation.
-

1. Select **Configure > Preferred Path**. The Configure Preferred Paths dialog box appears as shown in [Figure 68](#). The Configure Preferred Paths dialog box provides the configuration for a single switch's preferred path.

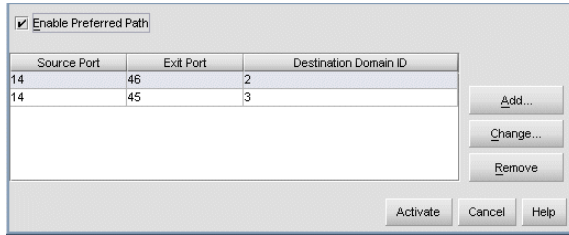


Figure 68 Configure Preferred Paths dialog box



NOTE: Some columns may only display when the FICON Management Style feature has been installed.

The columns included in the dialog box are as follows:

- **Source Port**—This column lists the source port of the preferred path.
- **Source Addr** (FICON management style only)—This column lists the source address of the preferred path.
- **Exit Port**—This column lists the exit port of the preferred path.
- **Exit Addr** (FICON management style only)—This column lists the exit address of the preferred path.
- **Destination Domain ID**—This column lists the domain ID of the destination switch or director. The range of the destination domain ID number is 1 through 31.



TIP: You may need to configure preferred paths on multiple switches or directors to optimize load balancing for an entire path between devices.



NOTE: A warning message will display if the switch or director has not been configured for insistent domain ID. If this is the case, close the dialog box and select **Configure > Operating Parameters > Switch Parameters**. Select the **Insistent** check box in the Configure Switch Parameters dialog box. Return to the Configure Preferred Paths dialog box and continue to [step 2](#).

2. Click **Add** to configure a new preferred path. The Add Preferred Path dialog box appears as shown in [Figure 69](#).

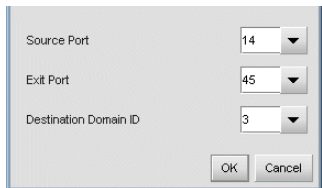

The image shows a dialog box titled "Add Preferred Path". It contains three labeled text boxes: "Source Port" with a dropdown menu showing "14", "Exit Port" with a dropdown menu showing "45", and "Destination Domain ID" with a dropdown menu showing "3". At the bottom right of the dialog box are two buttons: "OK" and "Cancel".

Figure 69 Add Preferred Path dialog box

3. Click the drop-down lists for the **Source Port**, **Exit Port**, and **Destination Domain ID** to make your choices. See ["Exporting the configuration report"](#) on page 122 for more information.

 **TIP:** You can also enter an exit port number for future or offline environments.

4. Click **OK**. The new route will be added to the table on the Configure Preferred Paths dialog box. The configuration will be validated.
5. Select the **Enable Preferred Paths** check box in the Configure Preferred Paths dialog box to enable the configured preferred paths. When this option is not selected, the preferred path configurations are not enforced, but the configured paths are retained for future use.
6. Click **Activate**.

Changing a preferred path

To change a preferred path, use the following steps:

1. Select **Configure > Preferred Path**. The Configure Preferred Paths dialog box appears as shown in [Figure 68](#).
2. To change a preferred path, select the path you want to change and click **Change**. The Change Preferred Path dialog box appears.
3. Change the data as required.
4. Click **Activate**. The data will be changed in the table on the Configure Preferred Paths dialog box.
5. Click the **Enable Preferred Paths** check box in the Configure Preferred Path to enable the configured preferred paths. When this option is not selected, the preferred path configurations are not enforced, but the configured paths are retained for future use.
6. Click **Activate**.

Removing a preferred path

To remove a new preferred path, use the following steps:

1. Select **Configure > Preferred Path**. The Configure Preferred Paths dialog box appears as shown in [Figure 68](#).
2. Select the path you want to remove and click **Remove**.
3. Click **Activate**.

Specifying preferred path example

Figure 70 shows a portion of a more complex SAN. In this example, we will do the following:

- Specify a path between the Source Device and Destination Device A, going through Switch 1, Switch 2, and Switch 3 (the desired data flow is shown as Data Flow 1).
- Enter data through port 14
- Exit data through port 45
- Make Switch 3 the destination device

Use the following procedure to accomplish the above tasks.

1. Select **Configure > Preferred Path** in Switch 1's Element Manager window to configure the path on Switch 1. The Add Preferred Path dialog box appears.
2. Click **14** in the **Source Port** field.
3. Click **45** in the **Exit Port** field.
4. Click **3** (Switch 3's domain ID) in the **Destination Domain ID** field.

This procedure only specifies that data will enter and exit Switch 1 through specific ports on its way to Switch 3. This process does not specify a Preferred Path for data moving through Switch 2. To specify paths through Switch 2 (Figure 71 on page 154), we will do the following:

- Enter data through port 11
- Exit data through port 21
- Make Switch 3 the destination device

Use the following procedure to accomplish the above tasks:

1. Select **Configure > Preferred Path** in Switch 2's Element Manager window to configure the path on Switch 2. The Add Preferred Path dialog box appears.
2. Click **11** in the **Source Port** field.
3. Click **21** in the **Exit Port** field.
4. Enter **3** (Switch 3's domain ID) in the **Destination Domain ID** field.

The primary choice for data movement will be from the Source Device in port 14 and out port 45 on Switch 1, in port 11 and out port 21 on Switch 2, and through Switch 3 to either Destination Device A or B.

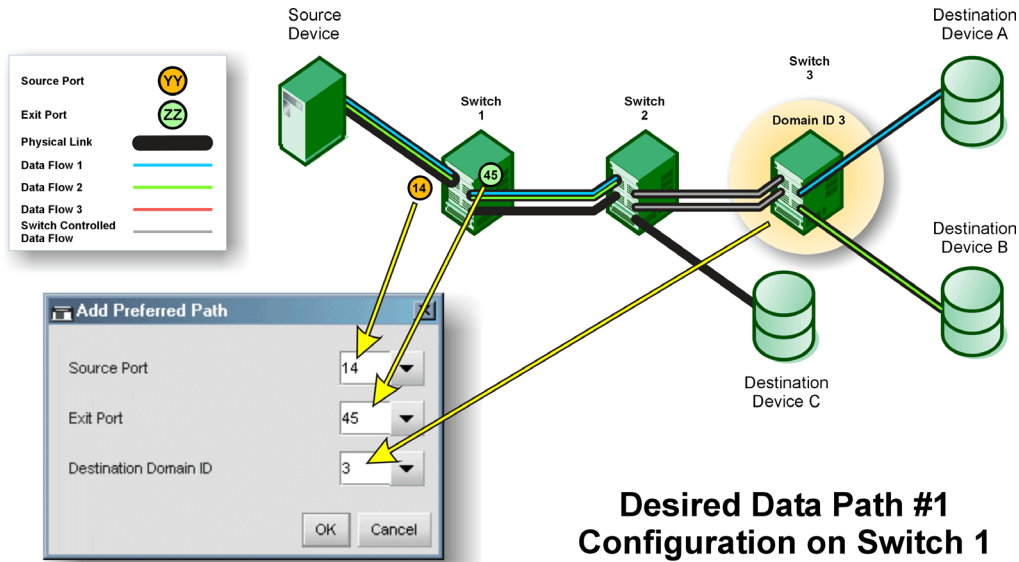


Figure 70 Specifying preferred path for switch 1

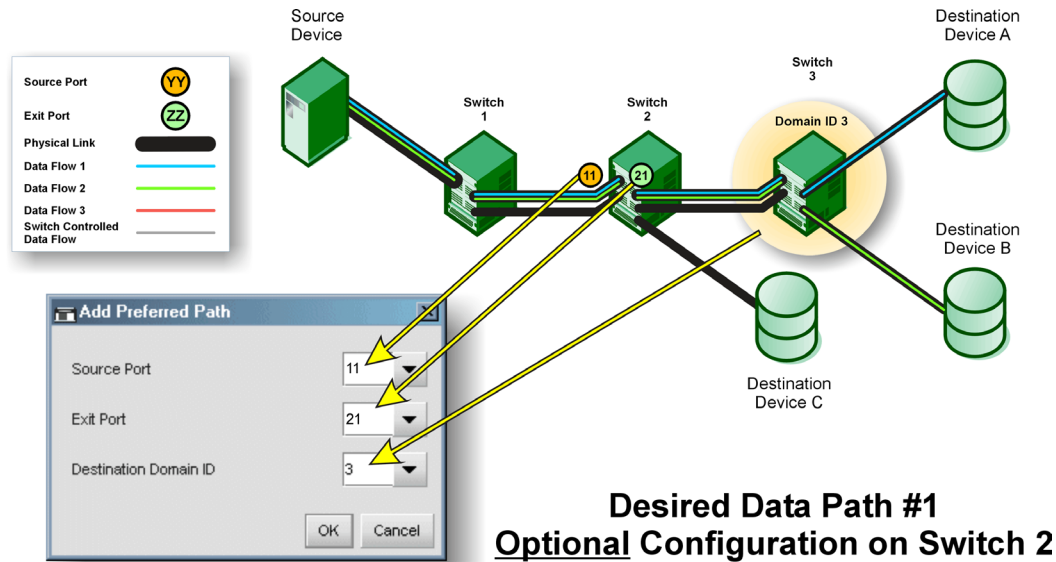


Figure 71 Specifying preferred path for switch 2

The following rules apply when configuring preferred paths:

- The switch's domain ID must be set to **insistent**.
- Domain IDs must be in the range of 1 through 31.
- The specified numbers for Source Ports and Exit Ports must be in the range equal to the number of ports for the switch being configured.
- For any source port, only one path may be defined to each destination domain ID.

To install and enable this option, select the **Features** option under the Element Manager's **Configure** menu. See "[Configuring a feature key](#)" on page 104.

FICON management server


The FICON Management Server is a keyed feature that allows host control and inband management of the director or switch through an IBM System/390 or zSeries 900 Parallel Enterprise Server attached to a director or switch port. The server communicates with the switch or director through a FICON channel. Control of connectivity and statistical product monitoring are provided through a host-attached console.

Installation

To install and enable this option, select the **Configure Feature Key** option under the Element Manager's **Configure** menu. Use steps under "[Configuring feature key](#)" on page 113.

Configuring the FICON management server

Use this procedure to configure whether the host is the controlling manager.

 **NOTE:** The optional FICON Management Server feature must be installed in order to perform this procedure.

Select **Configure > FICON Management Server**. The following options display:

- **Enable Management Server**—Adds a check mark and enable the management server. Click the check box to remove the check mark and disable this feature.
- **Parameters**—Click this option to display the Configure FICON Management Server dialog box, which includes the following options:
 - **Switch Clock Alert Mode**—Displays a check mark and enable clock alert mode. If this is enabled, the following occurs when users set the date and time through the Configure Date and Time dialog box (**Configure** menu):
 - If you enable **Periodic Date/Time Synchronization**, an error message appears indicating that Clock Alert Mode must be cleared to enable automatic synchronization of the date and time.
 - If you manually set the date and time (**Periodic Date/Time Synchronization** is not enabled), a confirmation dialog box will display. You must click **OK** on that dialog box to continue manual configuration.
 - **Host Control Prohibited**—Displays a check mark and prohibit a host management program from changing configuration and connectivity parameters on the director. In this case, the host program will have read authorization only and cannot make changes. When the check mark is not displayed, a host program can change configuration and connectivity parameters on the director.
 - **Programmed offline state control**—Displays a check mark and enable a host management program to control the director's offline and online state. When a check mark is not displayed, a host program cannot set the director online or offline.
- **Active=Saved**—Displays a check mark and enable the active=saved function for the IPL address configuration.

- If **Active=Saved** is enabled (check mark), the IPL and the active address configuration are maintained as identical configurations. If a new configuration is activated through the Configure Addresses - "Active" dialog box, that configuration becomes the IPL address configuration.
- If **Active=Saved** is not enabled (no check mark), the IPL address configuration and the active configuration are not maintained as identical and may, in fact, be different configurations. If the feature *is not* enabled, you can modify the IPL configuration through the Configure Addresses - "Active" dialog box. If the feature is enabled, the IPL file is locked to modification through the Configure Addresses - "Active" dialog box.
- **Code Page**—Consider the language required for the port name display that displays on the HAFM appliance. Language support is provided through character set 697 for all Extended Binary-Coded Decimal Interchange Code (EBCDIC) pages.

When planning the installation, select the EBCDIC code page for displaying host-assigned port names or the CUP name. As an example, if the code page for Italy is selected and a port name is assigned in Italian by the host management program, then the Italian language port name will display in the Element Manager.

This field lists the code pages that are available for configuration. The default code page is United States/Canada 00037. Refer to the following table for other code pages:

Table 8 Available code pages

Code Page Name	Code Page	Hexadecimal CPGID
United States/Canada	00037	0025
Germany/Austria	00273	0111
Brazil	00275	0113
Italy	00280	0118
Japan	00281	0119
Spain/Latin America	00284	011C
United Kingdom	00285	011D
France	00297	0129
International #5	00500	01F4

To configure FICON management server, use the following steps:

1. Select **Configure > Management Server** from the Element Manager menu bar. The Configure FICON Management Server dialog box appears.
2. Click the **Enable FICON** check box to enable the management server. (To disable the management server, click the check box again to remove the check mark.)

3. Select the **Parameters** option to open the Configure FICON Management Server Parameters dialog box, as shown in [Figure 72](#).



Figure 72 Configure FICON Management Server Parameters dialog box

4. Click the **Switch Clock Alert Mode** check box to enable or disable switch clock alert mode. When a check mark appears, the alert mode is enabled.
5. Click the **Host Control Prohibited** check box to allow or prohibit host control. When a check mark appears, host control is prohibited.
6. Click the **Programmed offline state control** check box to allow or prohibit offline state control. When a check mark appears, programmed control of the offline state is allowed.
7. Click the **Active=Saved** check box to enable or disable Active=Saved mode. When a check mark appears, the Active=Saved mode is enabled.
8. If necessary, select a code page from the **Code Page** drop-down list.
9. Click **Activate** to activate changes and close the dialog box.
10. If you are finished configuring the switch, back up the configuration data.

Open systems management server

The Open System Management Server (OSMS) is a keyed feature that allows host control and inband management of the director or switch through a management application that resides on an open-systems interconnection (OSI) device. This device is attached to a director or switch port. The device communicates with the switch or director through Fibre Channel common transport (FC-CT) protocol.

Installation

To install and enable this option, select the **Configure Feature Key** option under the Element Manager's **Configure** menu.

Configuring the open systems management server

Use these procedures to configure the Open Systems inband management program to function with the switch.

The optional Open Systems Management Server feature must be installed in order to perform this procedure.

To configure Open Systems Management Server, use the following steps:

1. Select **Configure > Management Server** from the **Element Manager** window. The Configure Open Systems Management Server dialog box appears.
2. Enable the management server when you click the **Enable Management Server** check box. (To disable the management server, click the check box again to remove the check mark.)
3. Click the check box in the **Host Control Prohibited** field to display a check mark and to prohibit the host management program from changing configuration and connectivity parameters on the switch. In this case, the host program has read-only access to configuration and connectivity parameters. Click the check box when it contains a check mark. This removes the check mark and allows a host program to change configuration and connectivity parameters on the switch.
4. To activate changes and close the dialog box, click **Activate**.
5. If you are finished configuring the switch, you can back up the configuration data.

SANtegrity features

SANtegrity includes a set of features that enhance security in SANs (Storage Area Networks) that contain a large and mixed group of fabrics and attached devices. Through these features, you can allow or prohibit switch attachment to fabrics and device attachment to switches. These features are enabled by purchasing a feature key, then enabling the key through the Configure Feature Key dialog box.

SANtegrity Binding features include:

- Fabric Binding
- Switch Binding

Enterprise Fabric Mode—Although this is not a keyed feature, the SANtegrity Fabric Binding and Switch Binding must be installed before you can use Enterprise Fabric Mode function through the **HAFM Fabrics** menu.

Fabric binding

This feature is managed through the **Fabric Binding** option, available through the **Fabrics** menu in HAFM when the **Fabrics** tab is selected. Using Fabric Binding, you can allow specific switches to attach to specific fabrics in the SAN. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

Online state functions

In order for Fabric Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the director or switch is offline or online. Be aware of the following:

- Because switches are bound to a fabric by World Wide Name (WWN) and domain ID, the **Insistent Domain ID** option in the Configure Switch Parameters dialog box is automatically enabled if Fabric Binding is enabled.
- If Fabric Binding is enabled and the switch is online, you cannot disable the Insistent Domain ID.
- If Fabric Binding is enabled and the director or switch is offline, you can disable the insistent domain ID, but this will disable Fabric Binding.
- You cannot disable Fabric Binding or Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.

Switch binding

This feature is managed through the **Switch Binding** submenu options available on the Element Manager **Configure** menu. Using **Switch Binding**, you can specify devices and switches that can attach to director and switch ports. This provides security in environments that include a large number of devices by ensuring that only the intended set of devices attach to a switch or director.

Configuring switch binding—overview

To configure Switch Binding, you must first activate the feature using the Switch Binding State Change dialog box while selecting the type of port where you want to restrict connection (connection policy). Possible selections are E_Ports, F_Ports, or all types.

If the director or switch is online, activating Switch Binding populates the Membership List in the Switch Binding - Membership List dialog box (Element Manager) with the following WWNs currently connected to the director or switch, depending on the connection policy set in the State Change dialog box:

- WWNs of devices connected to F_Ports (F_Port connection policy). The WWN is the WWN of the attached device's port.
- WWNs of switches connected to E_Ports (E_Port connection policy). The WWN is the WWN of the attached switch.
- WWNs of devices connected to F_Ports and switches connected to E_Ports (all-ports connection policy).

Notes

- When the Switch Binding feature is first installed and has not been enabled, the Switch Membership List is empty. When you enable Switch Binding, the Membership List is populated with WWNs of devices, switches, or both that are currently connected to the switch.
- If the switch is offline and you activate Switch Binding, the Membership List is not automatically populated.
- Edits to the Switch Binding Membership List will be maintained when you enable or disable Switch Binding.

After enabling Switch Binding, you prohibit devices and/or switches from connecting with director or switch ports by removing them from the Membership List in the Switch Binding Membership List dialog box. You allow connections by adding them to the Membership List. You can also add detached nodes and switches.

Enabling and disabling switch binding

1. Select **Configure > Switch Binding > Change State** from the **Element Manager** window. The Switch Binding State Change dialog box appears, as shown in [Figure 73](#).

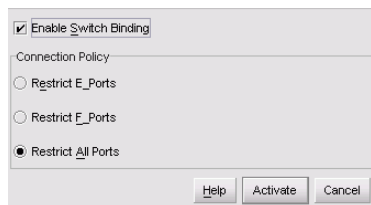


Figure 73 Switch Binding State Change dialog box

2. Perform one of the following steps:
 - To disable Switch Binding (a check mark appears in the **Enable Switch Binding** check box), click the **Enable Switch Binding** check box to remove the check mark, then click **Activate**.
 - To enable Switch Binding (check mark is not in the **Enable Switch Binding** check box), click the **Enable Switch Binding** check box to add a check mark. Go on to step 3 to set the Connection Policy.
3. Click one of the **Connection Policy** options.
 - **Restrict E_Ports**—Select this option if you want to restrict connections from specific switches to switch E_Ports. Switch WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection. Devices are allowed to connect to any F_Port.
 - **Restrict F_Ports**—Select this option if you want to restrict connections from specific devices to switch F_Ports. Device WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection. Switches are allowed to connect to any E_Port.
 - **Restrict All**—Select this option if you want to restrict connections from specific devices to switch F_Ports and switches to switch E_Ports. Device and switch WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection.
4. Click **Activate** to enable the changes and close the dialog box.
5. Edit the Switch Membership List through the Switch Binding Membership List dialog box to add or remove switches and devices that are allowed to connect with the switch.

Editing the switch membership list

1. Select **Configure > Switch Binding > Edit Membership List** from the Element Manager window. The Switch Binding Membership List dialog box appears, as shown in [Figure 74](#).
The WWNs of devices and/or switches that can currently connect to switch ports are listed in the **Switch Membership List** panel.

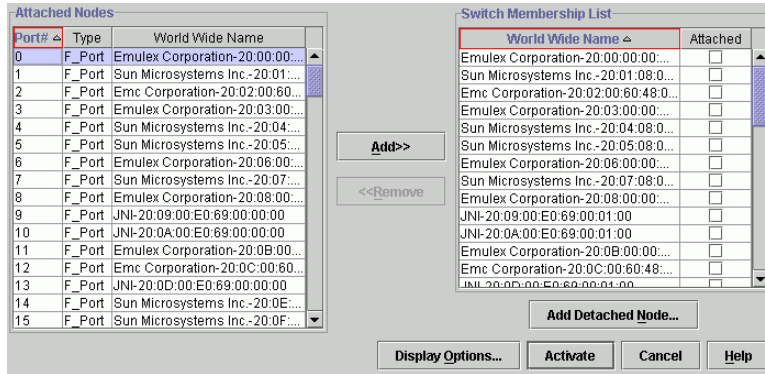


Figure 74 Switch Binding Membership List dialog box

See “This feature is managed through the Switch Binding submenu options available on the Element Manager Configure menu. Using Switch Binding, you can specify devices and switches that can attach to director and switch ports. This provides security in environments that include a large number of devices by ensuring that only the intended set of devices attach to a switch or director.” on page 160 for information on how the Switch Membership List is populated with WWNs according to options set in the Switch Binding State Change dialog box.

2. If nicknames are configured for WWNs through HAFM and you want these to display instead of WWNs in this dialog box, click **Display Options**. The Display Options dialog box appears.
3. Click **Nickname**, then click **OK**.
4. To prohibit connection to a switch port from a WWN currently in the Membership List, click the WWN or nickname in the **Membership List**, then click **Remove**. The WWN or nickname will move to the **Node List** panel. WWNs can only be removed from the fabric if any of the following is true:
 - The switch is offline.
 - Switch Binding is disabled.
 - The switch or device with the WWN is not connected to the switch.
 - Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the Switch Binding State Change dialog box. For example, a WWN for a switch attached to an E_Port can be removed if the Switch Binding Connection Policy was enabled to Restrict F_Ports.
 - The switch or device with the WWN is connected to a port that is blocked.
 - The switch or device with the WWN is not currently connected to the switch (detached node).

5. WWNs can be added to the **Switch Membership List** (and thereby allowed connection) when Switch Binding is either enabled or disabled. To allow connection to a switch port from a WWN in the **Node List** panel, select the WWN or nickname in the **Node List** panel, then click **Add**. The WWN or nickname will move to the **Membership List** panel.
6. To add a WWN for a device or switch not currently connected to the switch, click **Detached Node**. The Add Detached Node dialog box appears.
7. Enter the appropriate WWN or nickname (if configured through HAFM) and click **OK**. The WWN or nickname appears in the **Switch Membership List**.
8. Click **Activate** to enable the changes and close the dialog box.

Enabling and disabling and online state functions

In order for Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the director or switch is offline or online. Be aware of the following:

- Switch Binding can be enabled or disabled whether the switch is offline or online.
- Enabling Enterprise Fabric Mode automatically enables Switch Binding.
- You cannot disable Switch Binding if Enterprise Fabric Mode is enabled.
- If Enterprise Fabric Mode is enabled and the director or switch is online, you cannot disable Switch Binding. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.
- If Enterprise Fabric Mode is enabled and the director or switch is offline, you can disable Switch Binding, but Enterprise Fabric Mode will also disable.
- WWNs can be added to the Switch Membership List when Switch Binding is enabled or disabled.
- WWNs can only be removed from the Switch Membership List if any of the following are true:
 - The director or switch is offline.
 - Switch Binding is disabled.
 - The switch or device with the WWN is not connected to the director or switch.
 - Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the Switch Binding State Change dialog box. For example, a WWN for a switch attached to an E_Port can be removed if Switch Binding Connection Policy was enabled to Restrict F_Ports.
 - The switch or device with the WWN is connected to a port that is blocked.
 - The switch or device with the WWN is not currently connected to the director or switch (detached node).
- If the director or switch is online and Switch Binding is not enabled, all nodes and switches attached to the director or switch are automatically added to the Switch Membership List.

Zoning with switch binding enabled

Note that SANtegrity Binding has no effect on existing zoning configurations. However, note that if a device WWN is in a specific zone, but the WWN is not in the Switch Membership List, the

device cannot log in to the director or switch port and cannot connect to other devices in the zone with Switch Binding enabled.

Enterprise fabric mode

Enterprise Fabric Mode is an option available on the **Fabrics** menu in the HAFM application if the SANtegrity Binding feature key is installed. This option automatically enables the following features and operating parameters that are necessary in multiswitch Enterprise Fabric environments. Note that there are specific requirements for disabling these parameters and features when the director or switch is offline or online.

Features and parameters enabled

Fabric Binding

This is a SANtegrity Binding feature enabled through the **Fabrics** menu in HAFM that allows or prohibits switches and directors from merging with a selected fabric. See ["Enabling and disabling and online state functions"](#) on page 163 for details on enabling/disabling Fabric Binding with Enterprise Fabric Mode enabled.

Switch Binding

This is a SANtegrity Binding feature enabled through the **Configure** menu in the Element Manager that allows or prohibits switches and/or directors from connecting to switch E_Ports, devices from connecting to F_Ports. See ["Enabling and disabling and online state functions"](#) on page 163 for details on enabling/disabling Switch Binding with Enterprise Fabric Mode enabled.

Rerouting Delay

Rerouting delay is a parameter in the **Configure Switch Parameters** dialog box, available from the **Configure** menu in the Element Manager.

Rerouting Delay ensures that frames are delivered through the fabric in order to their destination. If there is a change to the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path. If Rerouting Delay is enabled, traffic ceases in the fabric for the time specified in the **E_D_TOV** field of the Configure Fabric Parameters dialog box (**Configure** menu). This delay enables frames sent on the old path to exit to their destination before new frames begin traversing the new path.

If Enterprise Fabric Mode is enabled, this parameter is automatically enabled and cannot be disabled unless the director or switch is offline. In this case, disabling Rerouting Delay also disables Enterprise Fabric Mode.

Domain RSCNs

This is a parameter in the Configure Switch Parameters dialog box, available from the **Configure** menu in the Element Manager. Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters and storage devices. As an example, this information might be that a logical path has

been broken because of a physical event, such as a fiber optic cable being disconnected from a port.

If Enterprise Fabric Mode is enabled, this parameter is automatically enabled and cannot be disabled unless the director or switch is offline. In this case, disabling domain RSCNs also disables Enterprise Fabric Mode.

Suppress Zoning RSCNs on Zone Set Activations

Fabric format domain register for state change notifications (RSCNs) are sent to ports on the switch following any change to the fabric's active zone set. These changes include activating and deactivating the zone set or enabling and disabling the default zone. When the **Suppress Zoning RSCNs on Zone Set Activations** check box is selected, fabric format RSCNs are not sent for zone changes to the attached devices on the switch. Click the check box to remove or add a check mark.

This option is disabled (check box not selected) by default. In most cases this option should be disabled so that attached devices can receive notification of zoning changes in the fabric. However, some HBAs may log out, then log back into the fabric when they receive an RSCN, thereby disrupting Fibre Channel traffic. Consult with your HBA and storage device vendor to determine if disabling this option (and thereby enabling RSCN transmission) will cause problems with your HBA or storage products.

Insistent Domain Identification (ID)

This is a parameter in the Configure Switch Parameters dialog box, available from the **Configure** menu in the Element Manager. Enabling this option sets the domain ID configured in the **Preferred Domain ID** field in the Configure Switch Parameters dialog box as the active domain identification when the fabric initializes. A static and unique domain identification is required by the Fabric Binding feature because the feature's Fabric Membership List identifies switches by WWN and domain ID. If a duplicate preferred domain ID is used, then insisted, warnings occur when directors and switches are added to a Fabric Membership List.

If Fabric Binding or Enterprise Fabric Mode is enabled, this option is automatically enabled and cannot be disabled unless these options are disabled when the director or switch is offline. If the director or switch is online, disabling Insistent Domain ID will disable Enterprise Fabric Mode and Fabric Binding.

Open trunking

Interswitch links (ISLs) connect ports between E_Ports on Fibre Channel switches and link these switches into a multiswitch fabric. Multiple ISLs may be connected between the switches in the fabric. Data from an attached end device (server or storage) flows through these ISLs to a target end-device connected to a switch somewhere in the fabric. A data flow is data received from a specified receive port that is destined for a port in a specified target domain (switch). The list of ISLs that are candidates for being rerouted (to or from) is derived from the fiber shortest path first (FSPF) algorithm.

The Open Trunking feature monitors the average data rates of all traffic flows on ISLs (from a receive port to a target domain), and periodically adjusts routing tables to reroute data flows from congested links to lightly loaded links and optimize bandwidth use. The objective of Open Trunking

is to make the most efficient possible use of redundant ISLs between neighboring switches, even if these ISLs have different bandwidths.

Load-balancing among the ISLs does not require user configuration, other than enabling Open Trunking. However, if desired, you can modify default settings for congestion thresholds (per port) and low BB_Credit threshold.

In particular, you do not need to manually configure ISLs into trunk groups of redundant links where data can be off-loaded. Candidate links for rerouting flow are identified and maintained automatically. This means that flow may be rerouted onto a link that goes to a different adjacent switch, as long as that link is on the least cost/shortest path to the destination domain ID.

To install and enable this option, select the **Configure Feature Key** option under the Element Manager's **Configure** menu. See "Configuring feature key" on page 113.

Enabling and configuring Open Trunking


To enable Open Trunking for a specific switch and configure threshold values and event notification options, use the following steps.

1. Select **Open Trunking** from the **Configure** menu. The Configure Open Trunking dialog box appears, as shown in Figure 75.

Port #	Use Algorithmic Threshold	Threshold %
0	<input checked="" type="checkbox"/>	66
1	<input checked="" type="checkbox"/>	66
2	<input checked="" type="checkbox"/>	66
3	<input checked="" type="checkbox"/>	66
4	<input checked="" type="checkbox"/>	66
5	<input checked="" type="checkbox"/>	66
6	<input checked="" type="checkbox"/>	66
7	<input checked="" type="checkbox"/>	66
8	<input checked="" type="checkbox"/>	66
9	<input checked="" type="checkbox"/>	66
10	<input checked="" type="checkbox"/>	66
11	<input checked="" type="checkbox"/>	66
12	<input checked="" type="checkbox"/>	66

Figure 75 Configure Open Trunking dialog box

2. Enable Open Trunking by clicking the **Enable Open Trunking** check box to display a check mark.
3. Set the **Congestion Thresholds** for ports as percentages of link bandwidths, in the range of 1% through 99%. These thresholds are used only when a port becomes an ISL. When the link's traffic load becomes greater than this percentage, the link is seen as *congested* and traffic is rerouted (if possible) to an uncongested link. Note that rerouting may not be possible if there are no alternate links available or if alternate links are congested or have no available BB_Credit.


 **NOTE:** Using default settings for port congestion thresholds should work well in most cases. Normally, you will not need to set them.

Set the **Congestion Threshold** using one of these methods:

- Click the check box under the **Use Algorithmic Threshold** column to display a value under the **Threshold %** column. This value is computed by the feature's rerouting algorithm. If you click this check box, you cannot enter a value into the **Threshold %** column for the port. If you click the check box to remove the check mark, any value that was set in the **Threshold %** column for the port will redisplay.
- Click in the **Threshold %** column and enter a value in the range of 1 through 99.

 **NOTE:** If no threshold is entered for a port, a default value is used that is based on port type (1 Gb/s or 2 Gb/s) and channel bandwidth. This field cannot be left blank.

4. Set **Event Notification** options.

 **NOTE:** If enabled, these notifications occur the first time the events occur. Notifications are not resent while the problem persists.


- **Unresolved Congestion.** Click this check box to display a check mark and enable notification. If enabled, an *unresolved congestion* entry is made to the Event Log and an SNMP trap will be generated, if trap recipients are configured through the Configure SNMP dialog box.

An unresolved congestion event occurs when the rerouting algorithm cannot find a path for rerouting data flow and relieving congestion on an ISL.

- **Back Pressure.** Click this check box to display a check mark and enable this option. If enabled, a back pressure entry will be made to the **Event Log**, and an SNMP trap will be generated if trap recipients are configured through the Configure SNMP dialog box.

A back pressure event occurs when the percentage of time the ISL has no available BB_Credit exceeds the Low BB_Credit threshold. A separate event also occurs when the back pressure condition ends.

5. Set the **Low BB_Credit Threshold**.

 **NOTE:** Using default settings for Low BB_Credit Threshold should work well in most cases. This step is not required.

This is the percentage of time that the transmitting link has no BB_Credit. This value is also used when determining routes for a transmit link. An ISL that has no BB_Credit for longer than this time percentage cannot be the recipient of traffic rerouted from other ISLs. Traffic on this ISL may be rerouted by Open Trunking, even if the ISL is not congested.

- Click **Default Threshold** and a default value (1 to 99%) will appear in the threshold field. If the default is enabled, you cannot enter values into the field.
- Click in the threshold field and enter a value from 1 to 99.

6. Click **Activate** to enable these values on the director and close the dialog box.

Pop-up menu

Right-click columns in the **Configuration Threshold** table to display menu options that globally change values in the column cells.

Use Algorithmic Threshold

Right-click in the column to display these options:

- **Set all to Default**—Adds check marks to all check boxes in this column and sets all cells of **Threshold %** column to default values.
- **Clear All**—Clears all check boxes in this column and restores values in cells of **Threshold %** column with previous values.

Threshold %

Right-click in the column to display these options:

- **Set All To xx**—Sets all cells in this column to the value (xx) that you clicked.
- **Restore All**—Sets all cells in the column to the previous values.

Open Trunking Log

The Open Trunking Log, as shown in [Figure 76](#) provides details on flow rerouting that is occurring through director ports.

Date/Time	Receive Port	Target Domain	Old Exit Port	New Exit P
Wed Sep 03 12:28...0	0	1	2	3
Wed Sep 03 12:28...1	1	2	3	4
Wed Sep 03 12:28...2	2	3	4	5
Wed Sep 03 12:28...3	3	4	5	6
Wed Sep 03 12:28...4	4	5	6	7

Export...

Clear

Refresh

Close

Help

Figure 76 Open Trunking Log

- **Date and Time**—Date and Time that action occurred.
- **Receive Port**—The decimal receive port number on the local switch associated with the flow that was rerouted.
- **Target Domain**—The decimal domain ID associated with the flow that was rerouted.
- **Old Exit Port**—The decimal exit port number on this switch that the flow used to get to the target domain.
- **New Exit Port**—The decimal exit port number on this switch that the flow now uses to get to the target domain.

A Information and error messages

This appendix lists information and error messages that display in pop-up message boxes from the HP StorageWorks HA-Fabric Manager (HAFM) application and the associated Element Managers.

The first section of the appendix lists HAFM application messages. The second section lists Element Manager messages. The text of each message is followed by a description and recommended course of action.

HAFM Application messages

Table 9 lists HAFM application information and error messages in alphabetical order.

Table 9 HAFM messages

Message	Description	Action
A zone must have at least one zone member.	When creating a new zone, one or more zone members must be added.	Add one or more zone members to the new zone using the Modify Zone dialog box.
A zone set must have at least one zone.	When creating a new zone set, one or more zones must be added.	Add one or more zones to the new zone set using the Modify Zone dialog box.
All alias, zone, and zone set names must be unique.	When creating a new alias, zone, or zone set, the name must be unique.	At the New Zone dialog box, select a unique name for the new alias, zone, or zone set.
All zone members are logged.	Attempt was made to display all zone members not logged in using the Zone Set tab, but all members are currently logged in.	Informational message.
An HAFM application session is already active from this workstation.	Only one instance of the HAFM application is allowed to be open per remote workstation.	Close all but one of the HAFM application sessions.
Are you sure you want to delete this network address?	The currently-selected network address will be deleted.	Click Yes to delete or No to cancel.
Are you sure you want to delete this nickname?	The selected nickname will be deleted from the list of nickname definitions.	Click Yes to delete the nickname or No to cancel the operation.
Are you sure you want to delete this product?	The selected product will be deleted from the list of product definitions.	Click Yes to delete the product or No to cancel the operation.
Are you sure you want to delete this user?	The selected user will be deleted from the list of user definitions.	Click Yes to delete the user or No to cancel the operation.
Are you sure you want to delete this zone?	The selected zone will be deleted from the zone library.	Click Yes to delete the zone or No to cancel the operation.
Are you sure you want to delete this zone set?	The selected zone set will be deleted from the zone library.	Click Yes to delete the zone set or No to cancel the operation.
Are you sure you want to overwrite this zone set?	The selected zone set will be overwritten in the zoning library.	Click Yes to overwrite or No to cancel.
Are you sure you want to remove all members from this zone?	All members will be deleted from the selected zone.	Click Yes to delete the members or No to cancel the operation.

Table 9 HAFM messages (continued)

Message	Description	Action
Cannot add a switch to a zone.	The device that you are attempting to add to the zone is a switch, which cannot be added to a zone.	Specify the port number or corresponding World Wide Name for the device you want to add to the zone.
Cannot connect to management server.	The HAFM application at a remote workstation could not connect to the HAFM appliance.	Verify the HAFM appliance internet protocol (IP) address is valid.
Cannot delete product.	The selected product cannot be deleted.	Verify the HAFM appliance-to-product link is up. If the link is up: <ul style="list-style-type: none"> • The HAFM appliance may be busy. • Another Element Manager instance may be open. • You may not have permission to delete the product.
Cannot disable Fabric Binding while Enterprise Fabric Mode is active.	You attempted to disable Fabric Binding through the Fabric Binding dialog box, but Enterprise Fabric Mode was enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box in the HAFM application before disabling Fabric Binding.
Cannot display route. All switches in route must be managed by the same server.	You cannot show the route between devices that are attached to switches or directors managed by a different HAFM appliance.	Make sure devices named in Show Routes dialog box are attached to products managed by this HAFM appliance.
Cannot display route. All switches in route must support routing.	You cannot show the route through a fabric that has switches or directors which do not support routing.	The route must contain only Edge Switch 2/16s, Edge Switch 2/32s, Director 2/64s, or Director 2/140s.
Cannot display route. Device is not a member of a zone in the active zone set.	You cannot show the route for a device that is not a member of a zone in the active zone set. The source node that you have selected is not part of a zone in the active zone set.	Enable the default zone or activate the zone for the device before attempting to show the route.
Cannot display route on one switch fabric.	You cannot show routes between end devices in a fabric when configuring Show Routes (Configure menu).	Error appears when attempting to show routes on a fabric with only one switch. Configure Show Routes on a multi-switch fabric.
Cannot display route. error 9.	An internal error has occurred while trying to view routes.	Contact the next level of support to report the problem.

Table 9 HAFM messages (continued)

Message	Description	Action
Cannot display route. No active zone enabled.	You cannot show the route through a fabric with no active zone.	Enable the default zone or activate a zone set before attempting to show the route.
Cannot have spaces in field.	Spaces are not allowed as part of the entry for this box.	Delete spaces from the field entry.
Cannot modify a zone set with an invalid name. Rename zone set and try again.	A zone set must have a valid name to be modified.	Assign a valid name to the zone set, then modify the name through the Modify Zone Set dialog box.
Cannot modify a zone with an invalid name. Rename zone and try again.	A zone must have a valid name to be modified.	Assign a valid name to the zone, then modify the name through the Modify Zone Set dialog box.
Cannot modify product.	The selected product cannot be modified.	Verify the HAFM appliance-to-product link is up. If the link is up: <ul style="list-style-type: none"> • The HAFM appliance may be busy. • Another Element Manager instance may be open. • You may not have permission to modify the product.
Cannot perform operation. Fabric is unknown.	No switches in the fabric are connected to the HAFM appliance.	Ensure at least one fabric-attached switch or director has an Ethernet connection to the HAFM appliance and retry the operation.
Cannot perform operation. The list of attached nodes is unavailable.	Attached nodes are unavailable and you attempt to modify a zone or create a new zone.	Verify an attached node is available and retry the operation.
Cannot remove all slot assignments from Partition 0.	You attempted to remove all slots from Partition 0, which would leave the partition disabled. Director firmware requires that Partition 0 is enabled.	Leave Partition 0 enabled.
Cannot retrieve current SNMP configuration.	The current SNMP configuration could not be retrieved.	Try again. If the problem persists, contact the next level of support.
Cannot save current SNMP configuration.	The current SNMP configuration could not be saved.	Try again. If the problem persists, contact the next level of support.
Cannot set write authorization without defining a community name.	An SNMP community name has not been configured.	Enter a valid community name in the Configure SNMP dialog box.

Table 9 HAFM messages (continued)

Message	Description	Action
Cannot show zoning library. No fabric exists.	You cannot show the zoning library if no fabric exists. You must have identified a switch or director to the <i>HAFM</i> application for a fabric to exist.	Identify an existing switch or director to the HAFM application using the New Product dialog box.
Click OK to remove all contents from log.	This action deletes all contents from the selected log.	Click OK to delete the log contents or Cancel to cancel the operation.
Connection to management server lost.	The connection to the remote HAFM appliance has been lost.	Log in to the HAFM appliance again through the HAFM Log In dialog box.
Connection to management server lost. Click OK to exit application.	The HAFM application at a remote workstation lost the network connection to the HAFM appliance.	Re-start the HAFM application to connect to the HAFM appliance.
Could not export log to file.	A log file input/output (I/O) error occurred and the file could not be saved to the specified destination. The disk may be full or write protected.	If the disk is full, use another disk. If the disk is write protected, change the write-protect properties or use another disk.
Default zoning is not supported in Open Fabric Mode.	A default zone cannot be enabled when the product is enabled for Open Fabric mode. Open Fabric mode does not support zone members defined by port numbers.	Change the Interop Mode from Open Fabric to Homogeneous using the Configure Fabric Parameters dialog box. You can also redefine zone members by the device WWN.
Device is not a member of a zone in the active zone set.	The selected device is not a member of a zone in the active zone set and therefore cannot communicate with the other devices in the route.	Enable the default zone or activate a zone set containing the member before attempting to show the route.
Download complete. Click OK and start the HAFM.	Download of HAFM and the Element Manager is complete.	Start the HAFM application to continue.
Duplicate community names require identical write authorizations.	If configuring two communities with identical names, they must also have identical write authorizations.	Verify that both communities with the same name have the same write authorizations.
Duplicate Fabric Name.	The specified fabric name already exists.	Select another name for the fabric.
Duplicate name in zoning configuration. All zone and zone set names must be unique.	Every name in the zoning library must be unique.	Modify (to make it unique) or delete the duplicate name.
Duplicate nickname in nickname configuration.	Duplicate nicknames cannot be configured.	Modify the selected nickname to make it unique.
Duplicate World Wide Name in nickname configuration.	A World Wide Name can be associated with only one nickname.	Modify (to make it unique) or delete the selected World Wide Name.
Duplicate zone in zone set configuration.	More than one instance of a zone is defined in a zone set.	Delete one of the duplicate zones from the zone set.

Table 9 HAFM messages (continued)

Message	Description	Action
Duplicate zone member in zone configuration.	More than one instance of a zone member is defined in a zone.	Delete one of the duplicate zone members from the zone.
Element Manager instance is currently open.	A product cannot be deleted while an instance of the Element Manager is open for that product.	Close the Element Manager, then delete the product.
Enabling this zone set will replace the currently active zone set. Do you want to continue?	Only one zone set can be active. By enabling the selected zone set, the current active zone set will be replaced.	Click OK to continue or Cancel to end the operation.
Error connecting to switch.	While viewing routes, the HAFM appliance was unable to connect to the switch. The switch failed or the switch-to-HAFM appliance Ethernet link failed.	Try the operation again. If the problem persists, contact the next level of support.
Error creating zone.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error creating zone set.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone set.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error reading log file.	The HAFM application encountered an error while trying to read the log.	Try the operation again. If the problem persists, contact the next level of support.
Error removing zone or zone member.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error transferring files < message >.	An error occurred while transferring files from the PC hard drive to the HAFM application. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.
Fabric Log will be lost once the fabric unpersists. Do you want to continue?	When you unpersist a fabric, the corresponding fabric log is deleted.	Click Yes to unpersist the fabric or No to cancel the operation.
Fabric member could not be found.	A fabric member does not exist when the application prepared to find a route, find a route node, or gather route information on that fabric member.	Ensure the product is incorporated into the fabric and retry the operation. If the problem persists, contact the next level of support.
Fabric not persisted.	You attempted to refresh or clear the log, after a fabric was unpersisted. When you unpersist a fabric, the corresponding fabric log is deleted.	Click OK to continue. Ensure the fabric is persisted before attempting to refresh or clear the Fabric Log.

Table 9 HAFM messages (continued)

Message	Description	Action
Field cannot be blank.	The data field requires an entry and cannot be left blank.	Enter appropriate information in the data field.
File transfer aborted.	You aborted the file transfer process.	Verify the file transfer is to be aborted, then click OK to continue.
HAFM error <error number 1 through 8 >.	The HAFM application encountered an internal error (1 through 8 inclusive) and cannot continue operation.	Contact the next level of support to report the problem.
Management server could not log you on. Verify your username and password.	An incorrect username or password (both case sensitive) was used while attempting to log in to the HAFM application.	Verify the username and password with the customer's network administrator and retry the operation.
Management server is shutting down. Connection will be terminated.	The HAFM application is closing and terminating communication with the attached product.	Reboot the HAFM appliance. If the problem persists, contact the next level of support.
Invalid character in field.	An invalid character was entered in the data field.	Remove invalid characters from the entry.
Invalid name.	One of the following invalid names was used: CON, AUX, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9, NUL, or PRN.	Select a valid name and retry the operation.
Invalid network address.	The IP address specified for the product is unknown to the domain name server (invalid).	Verify and enter a valid product IP address.
Invalid port number. Valid ports are (0-< nn >).	You have specified an invalid port number.	Specify a valid port number, in the range 0 to the maximum number of ports on the product minus 1. For example, for a switch with 32 ports, the valid port range is 0-31.
Invalid product selection.	At the New Product dialog box, an invalid product was selected.	Select a valid product and retry the operation.

Table 9 HAFM messages (continued)

Message	Description	Action
Invalid request.	<p>Three conditions result in this message:</p> <ul style="list-style-type: none"> You tried to add or modify a product from Product View and the network address is already in use. (Network addresses must be unique.) You tried to create a new user with a username that already exists. (A username must be unique.) You tried to delete the default Administrator user. (The default Administrator user cannot be deleted.) 	<p>Select the action that is appropriate to the activity that caused the error:</p> <ul style="list-style-type: none"> Network address: Specify a unique network address for the product. username: Specify a unique username for the new user ID. Do not delete the default Administrator user.
Invalid UDP port number.	The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from 1 through 65535 inclusive.	Verify and enter a valid UDP port number.
Invalid World Wide Name.	The specified World Wide Name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Enter a World Wide Name using the correct format.
Invalid World Wide Name or nickname.	The World Wide Name or nickname that you have specified is invalid. The valid format for the World Wide Name is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx). The valid format for a nickname is non blank characters, up to 32 characters.	Try the operation again using a valid World Wide Name or nickname.
Invalid World Wide Name. Valid WWN format is: xx:xx:xx:xx:xx:xx:xx:xx.	The specified World Wide Name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Retry the operation using a valid WWN or nickname.
Invalid zone in zone set.	The defined zone no longer exists and is invalid.	Delete the invalid zone from the zone set.
Limit exceeded.	You cannot add a new product or user to HAFM application if the maximum number of that resource already exists on the system.	Delete unneeded products or users from the system, before attempting to add any new ones.
No address selected.	You cannot complete the operation because an address has not been selected.	Select an address and retry the operation.

Table 9 HAFM messages (continued)

Message	Description	Action
No attached nodes selected.	An operation was attempted without an attached node selected.	Select an attached node and try the operation again.
No management server specified.	An HAFM appliance is not defined to the HAFM application.	At the HAFM 8 Log In dialog box, type an appliance name in the Server Name field and click Login .
No nickname selected.	No nickname was selected when the command was attempted.	Select a nickname and try again.
No Element Managers installed.	No director or switch Element Manager is installed on this workstation.	Install the appropriate Element Manager to this workstation.
No routing information available.	No information is available for the route selected.	Select a different route and try the operation again.
No user selected.	A user was not selected when the command was attempted.	Select a user and try again.
No zone member selected.	A zoning operation was attempted without a zone member selected.	Select a zone member and try the operation again.
No zone selected.	A zoning operation was attempted without a zone selected.	Select a zone and try the operation again.
No zone selected or zone no longer exists.	A zoning operation was attempted without a zone selected, or the zone selected no longer exists in the fabric.	Select a zone and try the operation again.
No zone set active.	A zone set cannot be deactivated if there are no active zones.	Informational message only—no action is required.
No zone set selected.	A zoning operation was attempted without a zone set selected.	Select a zone set and try the operation again.
No zone set selected or zone set no longer exists.	A zoning operation was attempted without a zone set selected, or the zone set you selected no longer exists in the fabric.	Select a zone set and try the operation again.
Only attached nodes can be displayed in this mode.	You cannot display unused ports when adding ports by World Wide Name.	Change the add criteria to Add by Port.
Password and confirmation don't match.	Entries in the password field and confirmation password field do not match. The entries are case sensitive and must be the same.	Enter the password and confirmation password again.
Remote sessions are not allowed from this network address.	Only IP addresses of remote workstations specified at the Remote Access dialog box are allowed to connect to the HAFM appliance.	Consult with the customer's network administrator to determine if the IP address is to be configured for remote sessions.

Table 9 HAFM messages (continued)

Message	Description	Action
Remote session support has been disabled.	The connection between the specified remote workstation and the HAFM appliance was disallowed.	Consult with the customer's network administrator to determine if the workstation entry should be modified at the Remote Access dialog box.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance may be busy. Try the operation again later.
Route data corrupted.	The information for this route is corrupt.	Try the operation again. If the problem persists, contact the next level of support.
Route request timeout.	The Show Route request timed out.	Try the operation again. If the problem persists, contact the next level of support.
Routing is not supported by the switch.	This switch or director does not support the Show Routes feature.	Select a different switch or director to show the route.
SANtegrity Feature not installed. Please contact your sales representative.	You selected Fabric Binding or Enterprise Fabric Mode from the Fabrics menu. These selections are not enabled because the optional SANtegrity binding feature is not installed.	Install the SANtegrity Binding feature to use Fabric Binding or enable Enterprise Fabric Mode.
Select alias to add to zone.	An alias was not selected before clicking Add .	Select an alias before clicking Add .
Selection is not a World Wide Name.	The selection made is not a World Wide Name.	Select a valid World Wide Name before performing this operation.
Server shutting down.	The HAFM application is closing and terminating communication with the attached product.	Reboot the HAFM appliance. If the problem persists, contact the next level of support.
SNMP trap address not defined.	If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined.	Enter a corresponding SNMP trap recipient address.
Switch is not managed by HAFM.	The selected switch or director is not managed by the HAFM application.	Select a different switch or director.
The Administrator user cannot be deleted.	The administrator user is permanent and cannot be deleted from the Configure Users dialog box.	Informational message only—no action is required.
The director did not handle the request	The director did not complete the action.	Try again. If the problem persists, contact your support representative.
The director is busy saving maintenance information.	The director is busy with a maintenance operation.	Try again. If the problem persists, contact your support representative.

Table 9 HAFM messages (continued)

Message	Description	Action
The director must be offline to change the Management Style.	You attempted to change management style with firmware level less than 6.0.	Select Set Online State from the Maintenance menu and then click Set Offline . You can then change the management style. Set the director back online when finished.
The director must be offline to configure.	You attempted a configuration change while the director was online.	Set the director offline and then perform the configuration change.
The Domain ID was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	You attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SAN Integrity Binding feature), but a switch already exists in the fabric with the same domain ID.	Enter a unique domain ID for the switch in the Add Detached Switch dialog box.
The management server is busy processing a request from another Element Manager.	The HAFM appliance is processing a request from another instance of an Element Manager and cannot perform the requested operation.	Wait until the process completes, then perform the operation again.
The link to the managed product is not available.	The Ethernet connection between the HAFM appliance and managed product is down or unavailable.	Establish and verify the network connection.
The maximum number of aliases has already been configured.	The maximum number of aliases allowed was reached.	Delete an existing alias before adding a new alias.
The maximum number of management server network addresses has already been configured.	The number of HAFM appliance IP addressees that can be defined to the HAFM application has already been configured.	Delete an existing IP address before adding a new address.
The maximum number of members has already been configured.	The maximum number of unique members is 4097. The maximum number of members is 8192.	Delete an existing zone member before adding a new zone member.
The maximum number of nicknames has already been configured.	The maximum number of nicknames that can be defined to the HAFM application was reached.	Delete an existing nickname before adding a new nickname.
The maximum number of open products has already been reached.	The maximum number of open switches allowed was reached.	Close an Element Manager session (existing open product) before opening a new session.
The maximum number of products has already been configured.	The number of managed HP switches (48) that can be defined to the HAFM application was reached.	Delete an existing product before adding a new product.
The maximum number of products of this type has already been configured.	The number of managed HP switches of this type (48) that can be defined to the HAFM application was reached.	Delete an existing product of this type before adding a new product.

Table 9 HAFM messages (continued)

Message	Description	Action
The maximum number of remote network addresses has already been configured.	A maximum number of eight IP addresses for remote workstations can be configured at the Session Options dialog box. That number was reached.	Delete an existing IP address before adding a new IP address.
The maximum number of users has already been configured.	The number of users (32) that can be defined to the HAFM application was reached.	Delete an existing user before adding a new user.
The maximum number of zones allowed has already been configured.	The maximum number of zones that can be defined was reached.	Delete an existing zone before adding a new zone.
The maximum number of zone sets has already been configured.	The maximum number of zone sets that can be defined was reached.	Delete an existing zone set before adding a new zone set.
The maximum number of zones per zone set has already been configured.	The maximum number of zones that can be defined in a zone set was reached.	Delete an existing zone before adding a new zone to the zone set.
The nickname does not exist.	The entered nickname does not exist in the fabric.	Configure the nickname to the appropriate product or select an existing nickname.
The nickname is already assigned. Either use a different name or do not save the name as a nickname.	The entered nickname already exists in the fabric. Each nickname must be unique.	Define a different nickname.
The software version on this management server is not compatible with the version on the remote management server.	A second HAFM appliance (client) connecting to the HAFM appliance must be running the same software version to log in.	Upgrade the software version on the downlevel HAFM appliance.
The zoning library conversion must be completed before continuing.	The zoning library conversion is incomplete and the requested operation cannot continue.	Complete the zoning library conversion, then retry the operation.
This fabric log is no longer valid because the fabric has been unpersisted.	The selected fabric log is no longer available because the fabric has been unpersisted.	To start a new log for the fabric, persist the fabric through the Persist Fabric dialog box.
This network address has already been assigned.	The specified IP address was assigned and configured. A unique address must be assigned.	Consult with the customer's network administrator to determine a new IP address to be assigned and configured.
This product is not managed by this management server.	The product selected is not managed by this HAFM appliance.	Select a product managed by this HAFM appliance or go to the HAFM appliance that manages the affected product.
This switch is currently part of this fabric and cannot be removed from the Fabric Membership List. Isolate the switch from the fabric prior to removing it from the Fabric Membership List.	You attempted to remove a switch from the Fabric Membership List using the Fabric Binding option, but the switch is still part of the fabric.	Remove the switch from the fabric by setting the switch offline or blocking the E_Port where the switch is connected.

Table 9 HAFM messages (continued)

Message	Description	Action
This World Wide Name was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	You attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity Binding feature), but an entry already exists in the Fabric Membership List with the same World Wide Name (WWN).	Enter a unique World Wide Name for the switch in the Add Detached Switch dialog box.
Too many members defined.	The maximum number of zone members that can be defined was reached.	Delete an existing zone member before adding a new zone member.
You do not have a compatible version of the management server software. In order for the HAFM application to function properly, a compatible version must be installed on the client machine. Click OK to install a compatible version.	The HAFM application version running on the HAFM appliance differs from the version running on the remote workstation (client). A compatible version must be downloaded from the HAFM appliance.	Download a compatible version of the HAFM application to the remote workstation (client) using the Web install procedure.
You do not have rights to perform this action.	Configured user rights do not allow this operation to be performed.	Verify user rights with the customer's network administrator and change as required using the Configure Users dialog box.
You must define an SMTP server address.	An SMTP server address must be defined and configured for e-mail to be activated.	Define the SMTP server address at the Configure E-Mail dialog box.
You must define at least one E-mail address.	At least one e-mail address must be defined and configured for e-mail to be activated.	Define an e-mail address at the Configure E-Mail dialog box.
You must define at least one remote network address.	At least one IP address for a remote workstation must be configured for a remote session to be activated.	Define an IP address for at least one remote workstation at the Remote Access dialog box.
You must download the HAFM client via the web install.	An attempt was made to download the HAFM application to a remote workstation (client) using an improper procedure.	Download a compatible version of the HAFM application to the remote workstation (client) using the Web install procedure.
Zones configured with port numbers are ignored in Open Fabric Mode.	While in Open Fabric mode, zones configured using port numbers are enforced through World Wide Names.	Informational message only—no action is required.

Table 9 HAFM messages (continued)

Message	Description	Action
Zones must be defined before creating a zone set.	You cannot create a zone set without any zones defined for HAFM.	Define zones using the New Zone dialog box.
Zoning by port number is ignored in Open Fabric Mode.	While in Open Fabric mode, zones configured using port numbers are enforced through World Wide Names.	Informational message only—no action is required.
Zoning by port number is not supported in Open Fabric Mode.	You cannot specify an item for zoning by port number if HAFM is in Open Fabric Mode.	Either define zones by WWN of device or change to Homogeneous Fabric mode in the Configure Operation Mode dialog box of the Element Manager.
Zoning name already exists.	Duplicate zone names are not allowed in the zoning library.	Modify (to make it unique) or delete the duplicate zone name.

Element Manager messages

Table 10 lists Element Manager information and error messages in alphabetical order

Table 10 Element Manager messages

Message	Description	Action
A Preferred Path already exists between this Source Port and this Destination Domain ID. Please re-configure the desired path.	For any source port, only one path may be defined to each destination domain ID.	On the Add/Change Preferred Path dialog box, change the preferred path.
Activating this configuration will overwrite the current configuration.	Confirmation to activate a new address configuration.	Click Yes to confirm activating the new address configuration or No to cancel the operation.
All configuration names must be unique.	All address configurations must be saved with unique names.	Save the configuration with a different name that is unique to all saved configurations.
All FPM ports will be held inactive while the director is configured to 2 Gb/sec speed. Do you want to continue?	Occurs when FPM cards are installed in the director and director speed is being set to 2 Gb/sec in the Configure Switch Parameters dialog box.	Replace FPM cards with UPM cards (UPM cards operate at 1 and 2 Gb/sec) or set the director speed to 1 Gb/sec.
All port names must be unique.	A duplicate Fibre Channel port name was configured. All port names must be unique.	Reconfigure the Fibre Channel port with a unique name.
All port names must be unique.	A duplicate port name was entered. Every configured port name must be unique.	Reconfigure the port with a unique name.
An Element Manager instance is already open.	Only one instance of the Element Manager can be open at one time.	Close the open Element Manager so the desired instance of the Element Manager can be opened.
Another Element Manager is currently performing a firmware install.	Only one instance of the Element Manager can install a firmware version to the director at a time.	Wait for the firmware installation process to complete and try the operation again.
Are you sure you want to delete firmware version?	This message requests confirmation to delete a firmware version. Firmware library can store up to 8 firmware versions.	Click Yes to delete the firmware version or No to abort the operation.
Are you sure you want to delete this address configuration?	Confirmation to delete the selected address configuration.	Click Yes to confirm the deletion of the address configuration or No to cancel the operation.

Table 10 Element Manager messages (continued)

Message	Description	Action
Are you sure you want to send firmware version?	This message requests confirmation to send a firmware version from the HAFM appliance's firmware library to the director. Firmware library can store up to 8 firmware versions.	Click Yes to send the firmware version or No to abort the operation.
Cannot change Port Type while Management Style is FICON without SANtegrity feature. Please contact your sales representative.	Firmware is below the required level and you attempted to change a port type in the Configure Ports dialog box while FICON management style, but the optional SANtegrity Binding feature is not installed.	Informational message. If the firmware is below the required level, install SANtegrity Binding before changing port types in the Configure Ports dialog box while in FICON management style.
Cannot create partition <partition_number> while FICON Management Server is enabled.	The user has moved slots into a partition while FMS Server is enabled.	Disable FMS Server before moving slots into a partition.
Cannot disable Switch Binding while Enterprise Fabric Mode is active and the switch is Online.	You attempted to disable Switch Binding through the Switch Binding Change State dialog box, but Enterprise Fabric Mode is enabled.	You must either disable Enterprise Fabric Mode using the Enterprise Fabric Mode dialog box in the HAFM application or set the switch offline before you can disable Switch Binding.
Cannot disable Insistent Domain ID while Fabric Binding is active.	You attempted to disable the Insistent Domain ID parameter through the Configure Switch Parameters dialog box, but Fabric Binding is enabled.	Disable Fabric Binding through the Fabric Binding dialog box before disabling these parameters.
Cannot enable beaconing on a failed FRU.	Occurs when selecting Enable Beaconing option for a failed FRU.	Replace FRU and enable beaconing again or enable beaconing on operating FRU.
Cannot enable beaconing while the system light is on.	Occurs when choosing Enable Beaconing option for a failed FRU.	Replace FRU and enable beaconing again or enable beaconing on an operating FRU.
Cannot enable beaconing while the system error light is on.	Beaconing cannot be enabled while the system error light is on.	Select Clear System Error Light from Product menu to clear error light, then enable beaconing.

Table 10 Element Manager messages (continued)

Message	Description	Action
Cannot enable Open Trunking while Enterprise Fabric Mode is active and the switch is offline.	Enterprise Fabric mode is active and the switch or director is online and you attempted to enable Open Trunking. This message only appears if the optional Open Trunking feature is installed.	<p>Perform either of the following steps:</p> <p>Disable Enterprise Fabric Mode option by selecting the appropriate fabric in the Fabric Tree portion of the HAFM Manager window (Fabrics tab) and then selecting Enterprise Fabric Mode from the Fabrics menu. When the Enterprise Fabric Mode dialog box appears, click Start and follow prompts to disable the feature.</p> <p>Set the switch or director offline through the Set Online State dialog box. Display this dialog box by selecting Set Online State from the Element Manager Maintenance menu.</p>
Cannot have E-Ports if Management Style is FICON unless SANtegrity feature is installed. Please contact your sales representative.	Firmware is below the required level and you attempted to change management style from Open Systems to FICON management style with E_Ports configured, but SANtegrity Binding is not installed.	Informational message. If firmware is below the required level and you install SANtegrity Binding before changing to FICON management style, then E_Ports will remain as E_Ports when you change to FICON management style. If SANtegrity Binding is not installed, setting a director to FICON management style will change all E_ports to G_Ports.
Cannot have spaces in field.	Spaces are not allowed as part of the entry for this field.	Delete spaces from the field entry.
Cannot install firmware to a director with a failed CTP card.	A firmware version cannot be installed on a director with a failed control processor (CTP) card.	Replace the failed CTP card and retry the firmware installation.
Cannot install firmware to a switch with a failed CTP card.	Firmware cannot be installed on a switch with a defective CTP card.	Note that the CTP card is not a FRU. If it fails, the switch must be replaced. After replacement, retry the firmware install to the switch.
Cannot modify director/switch speed. Ports speeds cannot be configured at a higher data rate than the director/switch speed.	Port speeds cannot be configured at a higher data rate than the director speed. This message appears when you set director speed to 1 GB/sec through the Configure Switch Parameters dialog box and at least one of the ports is running at 2 Gb/sec.	Either return the director speed to 2 Gb/sec or configure all port data speeds to 1 Gb/sec through the Configure Ports dialog box.

Table 10 Element Manager messages (continued)

Message	Description	Action
Cannot perform this operation while the director is offline.	This operation cannot take place while the director or switch is offline.	Configure the director or switch offline through the Set Offline State dialog box and then retry the operation.
Cannot retrieve current SNMP configuration.	The director SNMP configuration cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve diagnostics results.	Director diagnostic results cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve information for port.	Port information cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve port configuration.	The port configuration cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve port statistics.	Port statistics cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve switch date and time.	The director or switch date and time cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve switch state.	The director or switch state cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot run diagnostics on a port that is failed.	Port diagnostics (loopback tests) cannot be performed on a port that has failed any previous diagnostic (power-on diagnostic, online diagnostic, or loopback test). The amber LED associated with the port illuminates to indicate the failed state.	Reset the port and perform diagnostics again.
Cannot run diagnostics on an active E-port.	Port diagnostics cannot be performed on an active E-port.	Run diagnostics on an E-port only when it is not active.

Table 10 Element Manager messages (continued)

Message	Description	Action
Cannot run diagnostics on a port that is not installed.	Port diagnostics cannot be performed on a port card that is not installed.	Run diagnostics only on a port that is installed.
Cannot run diagnostics on a port card that is not installed.	Port diagnostics (loopback tests) cannot be performed on a port that does not have a small form factor (SFF) optical transceiver installed.	Install a transceiver in the port and perform diagnostics again.
Cannot run diagnostics while a device is logged-in to the port.	Port diagnostics (internal loopback test) cannot be performed on a port while an attached Fibre Channel device is logged in.	Ensure the device is logged out and perform diagnostics again.
Cannot run diagnostics while a device is logged-in to the port.	A device is logged in to the port where a diagnostic test is attempted.	Log out the device and run the diagnostic test again.
Cannot save IPL configuration while active=saved is enabled.	You cannot save the IPL file while the active=saved property is set.	The FICON Management Server property, active=save, must be disabled for HAFM to save the IPL file.
Cannot save port configuration.	The port configuration cannot be saved at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot save SNMP configuration.	The SNMP configuration cannot be saved at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set all ports to 1 Gb/sec due to speed restriction on some ports.	Appears if you try to set ports to operate at 1 Gb/sec data speed through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one configuration.
Cannot set all ports to 2 Gb/sec due to speed restriction on some ports.	Appears if you try to set ports to operate at 2 Gb/sec data speed through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one configuration.
Cannot set all ports to Negotiate due to port speed restriction on some ports.	You attempted to set all ports to Negotiate through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.

Table 10 Element Manager messages (continued)

Message	Description	Action
Cannot set director state.	The director state cannot be set because the link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set Fibre Channel parameters.	Fibre Channel parameters for the director cannot be set at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set switch date and time.	The switch date and time cannot be set at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set switch state.	The director or switch state cannot be set at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set write authorization without defining a community name.	A community name was not defined in the Configure SNMP dialog box for the write authorization selected.	Provide a name in the Name field where write authorization is checked.
Cannot start data collection.	The data collection procedure cannot be started by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot start firmware install while CTP synchronization is in progress.	The director's CTP cards are synchronizing and firmware cannot be installed until synchronization is complete.	Install the firmware after CTP card synchronization completes.
Cannot start port diagnostics.	Port diagnostics cannot be started at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot swap an uninstalled port.	A port swap cannot be performed when the port card is not installed.	Perform a swap only on a port that is installed.
Click OK to remove all contents from log.	This action deletes all contents from the selected log.	Click OK to delete the log contents or click Cancel to cancel the operation.
Connection to management server lost. Click OK to exit application.	The <i>HAFM</i> application at a remote workstation lost the network connection to the HAFM appliance.	Start the <i>HAFM</i> application to connect to the HAFM appliance.
Continuing may overwrite host programming. Continue?	Configurations sent from the host may be overwritten by HAFM.	Continuing will activate the current configuration, which may have been configured by a FICON host.

Table 10 Element Manager messages (continued)

Message	Description	Action
Could not export log to file.	A log file I/O error occurred and the file could not be saved to the specified destination. The disk may be full or write protected.	Ensure file name and drive are correct.
Could not find firmware file.	Firmware file selected was not found in the FTP directory. Or, the selected file is not a firmware file.	Ensure file name and directory are correct. Or, obtain a valid firmware file from your service representative.
Could not remove dump files from server.	Dump files could not be deleted from the HAFM appliance because the link may be down, or the HAFM appliance or Element Manager is busy.	Retry the operation later. If the condition persists, contact the next level of support.
Could not stop port diagnostics.	Port diagnostics could not be stopped by the Element Manager because the Ethernet link is down or busy, or because the director is busy.	Retry the operation later. If the condition persists, contact the next level of support.
Could not write firmware to flash.	A firmware version could not be written from the HAFM appliance to FLASH memory.	Retry the operation again. If the condition persists, contact the next level of support.
Control Unit Port (CUP) name and port name are identical (FICON ONLY).	Within the address configuration, one or more of the port names are the same as the CUP name.	Make sure all names are unique for the ports and CUP name.
Date entered is invalid.	The date is entered incorrectly at the Configure Date and Time dialog box. Individual field entries may be correct, but the overall date is invalid (for example, a day entry of 31 for a 30-day month).	Verify each entry is valid and consistent.
Device applications should be terminated before starting diagnostics. Press NEXT to continue.	Port diagnostics (loopback tests) cannot be performed on a port while an attached device application is running.	Terminate the device application and perform diagnostics again.
[device WWN] cannot be removed from the Switch Membership List while participating in Switch Binding. The device must be isolated from the switch, or Switch Binding deactivated before it can be removed.	You attempted to remove a device WWN from the Switch Membership List (SANTegrity Binding feature) while Switch Binding is enabled.	Remove the device from the switch by blocking the port, setting the switch offline, or disabling Switch Binding through the Switch Binding Change State dialog box before removing devices from the Switch Membership List.

Table 10 Element Manager messages (continued)

Message	Description	Action
Director clock alert mode must be cleared before enabling period synchronization.	Clock alert mode is enabled through the Configure FICON Management Server dialog box and you attempted to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box.	Disable clock alert mode through the Configure FICON Management Server dialog box.
Director must be offline to configure.	Clock alert mode is enabled through the Configure FICON Management Server dialog box and you attempted to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box.	Disable clock alert mode through the Configure FICON Management Server dialog box.
Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue?	Fabric Binding is enabled through HAFM and you attempted to disable Insistent Domain ID in the Configure Switch Parameters dialog box.	Click Yes if you want to continue and disable Fabric Binding.
Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue?	Fabric Binding is enabled through the HAFM and user attempted to disable Insistent Domain ID in the Configure Switch Parameters dialog box.	Click Yes if you want to continue and disable Fabric Binding.
Disabling Switch Binding will disable Enterprise Fabric Mode. Do you want to continue?	You attempted to disable Switch Binding through the Switch Binding State Change dialog box, but Enterprise Fabric Mode is enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box before disabling Switch Binding.
Do you want to continue with IPL?	This message requests confirmation to initial program load (IPL) the director.	Click Yes to IPL the director or Cancel to cancel the operation.
Domain IDs must be in the range of 1 to 31.	Domain IDs entered in the Configure Preferred Paths dialog box must fall in a specific range.	In the Configure Preferred Paths dialog box, change the number in the Destination Domain ID field to a number between 1 and 31, inclusive.
Duplicate Community names require identical write authorizations.	Duplicate community names are entered at the Configure SNMP dialog box, and have different write authorizations.	Delete the duplicate community name or make the write authorizations consistent.
Element Manager error <number>.	The Element Manager encountered an internal error and cannot continue.	Contact the next level of support to report the problem.
Element Manager instance is currently open.	A Element Manager window is currently open.	Informational message only.

Table 10 Element Manager messages (continued)

Message	Description	Action
Enterprise Fabric Mode will be disabled if any of the following parameters are disabled: Insistent Domain ID, Rerouting Delay, Domain RSCNs. Do you want to continue?	You attempted to disable these parameters in the Configure Switch Parameters dialog box while the switch was online, but Enterprise Fabric Mode (SANtegrity Binding feature) is enabled.	Click Yes if you want to continue, and disable Enterprise Fabric Mode.
Error retrieving port information.	An error occurred at the Element Manager while retrieving port information because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error retrieving port statistics.	An error occurred at the Element Manager while retrieving port statistics because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error stopping port diagnostics.	An error occurred at the Element Manager while attempting to stop port diagnostics from running because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error transferring files < message >.	An error occurred while transferring files from the PC hard drive to the Element Manager. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.
Exclusive management server connection to the director required for this command.	You attempted to execute a command that is not valid when more than one management server is connected to the director.	Exit the additional management servers so that only one is connected to the director.
Feature not supported. The 'product name' must be running version 05.00.00 or higher.	The firmware version on the hardware product (switch or director) is lower than 05.00.00. This message only appears if the optional Open Trunking feature is installed.	Install firmware version 5.00.00 or higher on the hardware product.
Field cannot be blank.	The data field requires an entry and cannot be left blank.	Enter appropriate information in the Data field.
Field has exceeded maximum number of characters.	The maximum number of data entry characters allowed in the field was exceeded.	Enter the information using the prescribed number of characters.
File transfer aborted.	You aborted the file transfer process.	Information message only.

Table 10 Element Manager messages (continued)

Message	Description	Action
File transfer is in progress.	A firmware file is being transferred from the HAFM appliance hard drive, or a data collection file is being transferred to a CD.	Informational message only—no action is required.
Firmware download timed out.	The director or switch did not respond in the time allowed. The status of the firmware install operation is unknown.	Retry the operation. If the problem persists, contact the next level of support.
Firmware file I/O error.	A firmware download operation aborted because a file I/O error occurred.	Retry the operation. If the problem persists, contact the next level of support.
Firmware file not found.	The firmware version is not installed (or was deleted) from the firmware library at the HAFM appliance.	Add the firmware version to the library and retry the operation.
Incompatible configuration between management style and management server.	If the Firmware is below the required level, only FICON management style is allowed if the FICON Management Server feature is enabled. You attempted to enable Open Systems management style.	Disable FICON Management Server, enable the Open Systems Management Server, or enable the Open Systems management style.
Incorrect product type.	When configuring a new product through the New Product dialog box, an incorrect product was specified.	Select the correct product type for the product with the network address.
Installing this feature key, while online, will cause an IPL operation on the switch and a momentary loss of LAN connection. This operation is non-disruptive to the Fibre Channel traffic. Do you wish to continue installing this feature key?	If the switch is online, installing the new feature key will cause an internal program load (IPL). The LAN connection to the HAFM appliance will be lost momentarily, but Fibre Channel traffic will not be affected.	Click Yes to install the feature key or No to not install.
Internal file transfer error received from director.	The director or switch detected an internal file transfer error.	Retry the operation. If the problem persists, contact the next level of support.
Invalid character in field.	An invalid character was entered in the Data field.	Remove invalid characters from the entry.
Invalid configuration name.	Attempted to save an address configuration name with an invalid name.	Use up to 24 alphanumeric characters, including spaces, hyphens, and underscores.

Table 10 Element Manager messages (continued)

Message	Description	Action
Invalid feature key.	The feature key was not recognized.	Re-enter the feature key. Ensure that you type each character in the correct case (upper or lower), include the dashes, and do not add any spaces at the end.
Invalid firmware file.	The file selected for firmware download is not a firmware version file.	Select the correct firmware version file and retry the operation.
Invalid management server address.	The IP address specified for the HAFM appliance is unknown to the domain name server (invalid).	Verify and enter a valid HAFM appliance IP address.
Invalid network address.	The IP address specified for the product is unknown to the domain name server (invalid).	Verify and enter a valid product IP address.
Invalid port address.	Invalid port address has been entered.	Verify port address through the Configure Addresses—"Active" dialog box (FICON management style only) and re-enter.
Invalid port number.	The port number must be within a range of ports for the specific director or switch model.	Enter a port number within the correct range.
Invalid port swap.	Port swap selection is not allowed.	Ensure that each port selected for swap has not been previously swapped.
Invalid response received from switch.	An error occurred at the switch during a firmware download operation.	Retry the firmware download operation. If the problem persists, contact the next level of support.
Invalid response received from director.	An error occurred at the director during a firmware download operation.	Retry the firmware download operation. If the problem persists, contact the next level of support.
Invalid serial number for this feature key.	The serial number and the feature key did not match.	Ensure that the feature key being installed is specifically for this director serial number.
Invalid UDP port number.	The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from 1 through 65535 inclusive.	Verify and enter a valid UDP port number from 1 through 65535.
Invalid value for BB_Credit.	At the Configure Fabric Parameters dialog box, the buffer-to-buffer credit (BB_Credit) value must be an integer from 1 through 60 inclusive.	Verify and enter a valid number between 1 through 60.

Table 10 Element Manager messages (continued)

Message	Description	Action
Invalid value for Low BB Credit threshold (1-99) %.	Low BB Credit Threshold field in Configure Open Trunking dialog box must have entries in the range from 1 and 99. This message only appears if the optional Open Trunking feature is installed.	Enter a value from 1 to 99 into the Low BB Credit Threshold field of the Configure Open Trunking dialog box.
Invalid value for day (1-31).	At the Configure Date and Time dialog box, the DD value (day) must be an integer from 1 through 31 inclusive.	Verify and enter a valid date.
Invalid value for E_D_TOV.	At the Configure Fabric Parameters dialog box, the error detect time-out value (E_D_TOV) must be an integer from 2 through 600 inclusive.	Verify and enter a valid number.
Invalid value for hour (0-23).	At the Configure Date and Time dialog box, the HH value (hour) must be an integer from 0 through 23 inclusive.	Verify and enter a valid time.
Invalid value for minute (0-59).	At the Configure Date and Time dialog box, the MM value (minute) must be an integer from 0 through 59 inclusive.	Verify and enter a valid time.
Invalid value for month (1-12).	At the Configure Date and Time dialog box, the MM value (month) must be an integer from 1 through 12 inclusive.	Verify and enter a valid date.
Invalid value for R_A_TOV.	At the Configure Fabric Parameters dialog box, the resource allocation time-out value (R_A_TOV) must be an integer from 10 through 1200 inclusive.	Verify and enter a valid number.
Invalid value for second (0-59).	At the Configure Date and Time dialog box, the SS value (second) must be an integer from 0 through 59 inclusive.	Verify and enter a valid time.

Table 10 Element Manager messages (continued)

Message	Description	Action
Invalid value for threshold (1-99)%.	Value entered for each port in the Configure Open Trunking dialog box must be in the range from 1 to 99. This message only appears if the optional Open Trunking feature is installed.	Enter a number from 1 to 99 into the Threshold % column of the Configure Open Trunking dialog box.
Invalid value for year.	At the Configure Date and Time dialog box, the YYYY value (year) must be a four-digit value.	Verify and enter a four-digit value for the year.
Invalid World Wide Name or nickname.	The World Wide Name or nickname that you have specified is invalid. The valid format for the World Wide Name is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx). The valid format for a nickname is non blank characters, up to 32 characters.	Try the operation again using a valid World Wide Name or nickname.
Link dropped.	The HAFM appliance-to-director Ethernet link was dropped.	Retry the operation. Link re-connects are attempted every 30 seconds. If the condition persists, contact the next level of support.
Log is currently in use.	Access to the log is denied because the log was opened by another instance of the Element Manager.	Retry the operation later. If the condition persists, contact the next level of support.
Loopback plug(s) must be installed on ports being diagnosed. Press Next to continue.	External loopback diagnostics require an optical loopback plug to be installed.	Ensure that an optical loopback plug is installed in port optical transceiver before running external wrap diagnostic testing.
Maximum number of versions already installed.	The number of firmware versions that can be defined to the HAFM application's firmware library (eight) was reached.	Delete an existing firmware version before adding a new version.
No file was selected.	Action requires the selection of a file.	Select a file.
No firmware version file was selected.	A file was not selected in the Firmware Library dialog box before an action, such as modify or send was performed.	Click on a firmware version in the dialog box to select it, then perform the action again.
No firmware versions to delete.	There are no firmware versions in the firmware library to delete, therefore the operation cannot be performed.	Informational message only—no action is required.

Table 10 Element Manager messages (continued)

Message	Description	Action
Nonredundant director must be offline to install firmware.	For directors, if the director has only one CTP card, the director must be set offline to install a firmware version. For switches, since the switch has only a single CTP card, it must be offline to initiate a firmware installation. Note that the CTP card is an internal component and not a FRU.	Set the director or switch offline and install the firmware.
Not all of the optical transceivers are installed for this range of ports.	Some ports in the specified range do not have optical transceivers installed.	Use a port range that is valid for the ports installed.
Open Trunking is not installed for this product. Please contact your sales representative.	The Open Trunking feature key has not been enabled. This message only appears if the optional Open Trunking feature is installed.	Enter the feature key into the Configure Feature Key dialog box and enable the key. If you require a feature key, see your account representative.
Performing this operation will change the current state to Offline.	This message requests confirmation to set the director offline.	Click OK to set the director offline or click Cancel to cancel the operation.
Performing this operation will change the current state to Online.	This message requests confirmation to set the director online.	Click OK to set the director online or click Cancel to cancel the operation.
Performing this action will overwrite the date/time on the switch.	Warning that occurs when configuring the date and time through the Configure Date and Time dialog box, that the new time or date will overwrite the existing time or date set for the director or switch.	Verify that you want to overwrite the current date or time.
Periodic Date/Time synchronization must be cleared.	Action cannot be performed because Periodic Date/Time Synchronization option is active.	Click Periodic Date/Time Synchronization check box in Configure Date and Time dialog box (Configure menu) to clear check mark and disable periodic date/time synchronization.
Port binding was removed from attached devices that are also participating in Switch Binding.	Informational message. You removed Port Binding from attached devices, but one or more of these devices is still controlled by Fabric Binding.	Review the Switch Binding Membership List to determine if the devices should be members.
Port cannot swap to itself.	Port addresses entered in the Swap Ports dialog box are the same.	Ensure that address in the first and second Port Address fields are different.
Port diagnostics cannot be performed on an inactive port.	This appears when port diagnostics is run on a port in an inactive state.	Run the diagnostics on an active port.

Table 10 Element Manager messages (continued)

Message	Description	Action
Port speeds cannot be configured at a higher rate than the director speed.	This appears when you configure a port to 2 Gb/sec and the director speed is set to 1 Gb/sec.	Set the director speed to 2 Gb/sec in the Configure Switch Parameter dialog box.
Port numbers must be in the range of 0 to xxx.	When configuring Preferred Paths, source ports and exit ports must be in the range of ports for the switch being configured.	In the Configure Preferred Paths dialog box, change the numbers in the Source Port and Exit Port fields to fall within the port count of the switch on which you are configuring paths.
Preferred Paths can not be enabled until the Domain ID is set to Insistent. Disable Preferred Paths, then configure Switch Parameters.	If the switch's domain ID has not been set to Insistent, the user is not allowed to activate the Preferred Path configuration with the Enable Preferred Paths check box selected.	Close the Configure Preferred Paths dialog box and click Configure > Operating Parameters > Switch Parameters . In the Configure Switch Parameters dialog box, click the Insistent check box.
R_A_TOV must be greater than E_D_TOV.	R_A_TOV must be greater than E_D_TOV.	Change one of the values so that R_A_TOV is greater than E_D_TOV
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify that the Ethernet connection between the HAFM appliance and the director is up or available.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify that the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance may be busy. Try the operation again later.
SANtegrity Feature not installed. Please contact your sales representative.	You selected Switch Binding from the Configure menu, but the optional SANtegrity Binding feature is not installed.	Install the SANtegrity Binding key through the Configure Feature Key dialog box before using Switch Binding features.
Send firmware failed.	A firmware download operation failed.	Retry the firmware download operation. If the problem persists, contact the next level of support.
SNMP trap address not defined.	If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined.	Enter a corresponding SNMP trap recipient address.
Stop diagnostics failed. The test is already running.	Diagnostics for the port was not running and Stop was selected on the Port Diagnostics dialog box. Diagnostics quit for the port for some reason, but Stop remains enabled.	Verify port operation. Retry diagnostics for the port and select Stop from the dialog box. If problem persists, contact the next level of support.

Table 10 Element Manager messages (continued)

Message	Description	Action
Stop diagnostics failed. The test was not running.	This action failed because the test was not running.	Informational message.
Switch Binding was removed from attached devices that are also participating in Port Binding. Please review the Port Binding Configuration.	The device WWNs were removed from the director's Switch Membership List (SANtegrity Binding feature), but you should note that one or more of these devices still has security control in port binding.	Verify that the security level for each device is as required by reviewing the Bound WWN list in the Configure Ports dialog box.
System diagnostics cannot run. The Operational Status is invalid.	System diagnostics cannot run on switches with failed ports	Replace failed ports.
Switch clock alert mode must be cleared before enabling period synchronization.	Clock alert mode is enabled through the Configure FICON Management Server dialog box and user is attempting to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box.	Disable clock alert mode through the Configure FICON Management Server dialog box.
The add firmware process has been aborted.	You aborted the process to add a firmware version to the HAFM appliance's firmware library.	Verify the firmware addition is to be aborted, then click OK to continue.
The data collection process failed.	An error occurred while performing the data collection procedure.	Try the data collection procedure again. If the problem persists, contact the next level of support.
The data collection process has been aborted.	You aborted the data collection procedure.	Verify the data collection procedure is to be aborted, then click OK to continue.
The default zone must be disabled to configure.	The message appears when you attempted to change the management style to Open Fabric and the default zone is enabled.	Disable the default zone and repeat the operation.
The Ethernet link dropped.	The Ethernet connection between the HAFM appliance and the director is down or unavailable.	Establish and verify the network connection.
The firmware file is corrupted.	A firmware version file is corrupt.	Contact the next level of support to report the problem.
The firmware version already exists.	This firmware version already exists in HAFM appliance's firmware library.	Informational message only—no action is required.

Table 10 Element Manager messages (continued)

Message	Description	Action
The following parameters cannot be disabled while Enterprise Fabric Mode is active: Insistent Domain ID, Rerouting Delay, Domain RSCNs.	You attempted to disable these parameters in the Configure Switch Parameters dialog box while Enterprise Fabric Mode is enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box in HAFM, then disable the parameters.
The link to the director is not available.	The Ethernet connection between the HAFM appliance and the director is down or unavailable.	Establish and verify the network connection.
The link to the switch is not available.	The Ethernet connection between the HAFM appliance and the switch is down or unavailable.	Establish and verify the network connection.
The IPL configuration cannot be deleted.	Deletion of the IPL address configuration was attempted and was not allowed.	Cancel the operation.
The management server is busy processing a request from another Element Manager.	The HAFM appliance is processing a request from another instance of an Element Manager, and cannot perform the requested operation.	Wait until the process is completes, then perform the operation again.
The optical transceiver is not installed.	Information is not available for a port without an optical transceiver installed.	Install an SFP optical transceiver in the port.
The switch did not accept the request.	The director or switch cannot perform the requested action.	Retry the operation. If the condition persists, contact the next level of support.
The maximum number of address configurations has been reached.	The maximum number of saved address configurations has been reached.	Delete configurations no longer needed to allow new configuration to be saved.
The switch did not respond in the time allowed.	While waiting to perform a requested action, the director or switch timed out.	Retry the operation. If the condition persists, contact the next level of support.
The switch is busy saving maintenance information.	The director or switch cannot perform the requested action because it is busy saving maintenance information.	Retry the operation later. If the condition persists, contact the next level of support.
The switch must be offline to change the Management Style.	The firmware is below the required level and you attempted to change the management style.	Select Set Online State from the Maintenance menu and click Set Offline . Then change the management style. Set the director or switch back online when finished.

Table 10 Element Manager messages (continued)

Message	Description	Action
The switch must be offline to configure.	A configuration changed was attempted for a configuration requiring offline changes.	Take the appropriate actions to set the director or switch offline before attempting the configuration change.
This feature is not installed. Please contact your sales representative.	This feature has not been installed.	Contact your sales representative.
This feature key does not include all of the features currently installed and cannot be activated while the switch is online.	The feature set currently installed for this system contains features that are not being installed with the new feature key. To activate the new feature key, you must set the switch offline. Activating the new feature set, however, will remove current features not in the new feature set.	Set the switch offline through the Set Online State dialog box, then activate the new feature key using the Configure Feature Key dialog box. The new feature key will display both the new features and the features that were installed previously.
This feature key does not include all of the features currently installed. Do you want to continue with feature key activation?	The feature set currently installed for this system contains features that are not being installed with the new feature key.	Click Yes to activate the feature key and remove current features not in the new feature set or No to cancel.
Threshold alerts are not supported on firmware earlier than 01.03.00.	Threshold alerts are not supported on firmware earlier than 01.03.00.	Informational message.
Unable to change incompatible firmware release.	You tried to download a firmware release that is not compatible with the current product configuration.	Refer to the product release notes or contact the next level of support to report the problem.
Unable to save data collection file to destination.	The HAFM appliance could not save the data collection file to the specified location (PC hard drive, CD, or network).	Retry the operation. If the condition persists, contact the next level of support.
You do not have rights to perform this action.	Configured user rights do not allow this operation to be performed.	Verify user rights with the customer's network administrator and change as required.

Index

10-100 km configuration, port properties dialog box 66

A

acronyms, FRU 130
active addresses 27
active zone set state, default value 148
active=saved 156
address 31
address configuration library dialog box 110
address configurations, stored, managing 110
address ID errors 82
addresses
 director, default values 147
 FICON management style 27
 port 75
 port list view 72
alerts
 link incident (LIN)
 configuring 99
 description 87
 threshold 28
 clearing 71
 configuring 117
Alternate Control Prohibited (ACP) enabling 124
ASCII format for logs 125
attached WWN option button 70
attachment
 invalid
 list of reasons 67
 port state 86
 port binding error 66
audience 11
audit log 29
 capacity 125
 description 127
authorization traps, enabling 112
authorized reseller, HP 13

B

backing up and restoring
 configuration 144
 configuration data 124
 element manager data 47
backup and restore configuration dialog box 145
bar graph 80
 performance view 79
BB_Credit 76, 95
 default value 147
 extended distance buffering 98
beaconing
 enabling 69
 for CTP card 62
 for FPM card 61
 for SBAR card 62
 for unit 59
 port properties dialog box 66
 port state 86
 SBAR card indicator 56
bind port dialog box 70
binding, port, error 67
bit-error threshold 132
block all ports dialog box, displaying 61, 68
block configuration, port properties dialog box 65
blocked states, port 72
blocking ports 98
 FICON management style 108, 109
bound WWN
 configure ports dialog box 100
 port binding dialog box 70
buffer-to-buffer credit
 default value 147
 node properties dialog box 78
button functions, performance view 84

C

call-home notification, enabling 31, 144
channel wrap test
 description 70
 ports 74

- circle, green
 - meaning of 43
 - port 63
- class 2 statistics table 81
- class 3 statistics 81
- class of service, node properties dialog box 78
- clear system error light
 - product menu 25
- clearing link incident alerts 70
- clearing port counters 41, 44
- close product menu 25
- closing the element manager 44
- code pages 157
- collect maintenance data option 140
- collecting maintenance data 140
- component status, monitoring 53
- configuration changes, audit log 127
- configuration data
 - backing up and restoring 124, 144
 - default configuration values 147
 - resetting 146
- configuration report 122
- configurations
 - backing up and restoring 32
 - resetting 32, 146
- configure
 - Alternate Control Prohibited (ACP) 124
 - Preferred Path 152
 - RX BB Credit 98
 - zoning 145
- configure addresses - "active" 109
- configure addresses - "active" dialog box 109
- configure addresses, stored option 110
- configure date and time (manually) dialog box 60
- configure date and time dialog box 28
- configure date and time periodic synchronization dialog box 60
- configure fabric parameters dialog box 95
- configure feature key dialog box 28, 113
- configure FICON management server dialog box 157
- configure FICON management server parameters dialog box 158
- configure identification dialog box 25, 90
- configure management style 103
 - FICON procedure 105
 - Open Systems management style procedure 103
- configure menu 25
 - addresses - "active" 109
 - backup and restore configuration 124
 - configure threshold alert(s) 117
 - date/time 28, 115
 - enable telnet 29
 - enable web server 29
 - export configuration report 29, 122
 - features 28
 - identification 25
 - ports 27, 97
 - Preferred Path 26
 - SNMP agent 27
 - switch binding 26, 162
 - threshold alert(s) 28
- Configure Open Systems Management Server dialog box 159
- configure Open Trunking
 - pop-up menu 168
- configure open trunking dialog box 166
- configure open trunking dialog box menu 168
- configure ports dialog box 27, 97, 103
 - blocking ports 72
 - FICON management style 105
 - menu options 101
 - open systems management style 103
- configure SNMP
 - dialog box 112
- configure SNMP dialog box 27, 112
- configure switch parameters dialog box 91
- configure threshold alerts, procedure 117
- configuring
 - date and time 28
 - procedure 115
 - fabric operating parameters 95
 - feature key 113
 - FICON management server 113
 - identification 90
 - Open Systems Management Server 113
 - port addresses 108
 - port speeds 94
 - ports, FICON management style 105
 - preferred paths 150
 - RX BB Credit 98
 - switch operating parameters 91
- configuring features, menu option 28
- connection failure, port binding 100

- control unit port (CUP) name 109
- conventions
 - document 12
 - text symbols 12
- cooling fan module, failure indicator 56
- copy address configuration dialog box 111
- counters, port, clearing 41, 44
- CPGID, code pages 157
- CRC errors 82
- CTP card
 - active indicator 55
 - beaconing, enabling 62
 - failure indicator 55
 - FRU properties 62
 - IML 141
 - IPL 141
 - menu 35
 - properties 35
 - switchover 62
- CTP card menu 62
- CUP name
 - assigning 109
 - description 109
- current IP address, director 146
- cyclic redundancy checks, errors 82

D

- data collection option 31
- data default values table 147
- data field size, node properties dialog box 78
- data, backing up and restoring 47
- date and time, configuring 115
- date/time periodic synchronization feature 60
- defaults
 - call-home notification 144
 - code page 157
 - configuration data 146
 - data, table of values 147
 - enable e-mail notification 31
 - LIN alerts 99
 - switch priority setting 96
- define nickname dialog box, displaying 76
- degraded operation, event log 128
- delimiter errors 82
- diagnostics, port 61, 68

- dialog boxes 168
 - address configuration library 110
 - backup and restore configuration 145
 - block all ports 61, 68
 - configure addresses - "active" 109
 - configure date and time (manually) 60
 - configure date and time periodic synchronization 60
 - configure fabric parameters 95
 - configure feature key 28, 113
 - configure FICON management server 157
 - configure FICON management server parameters 158
 - configure identification 25, 90
 - Configure Open Systems Management Server 159
 - configure Open Trunking 166
 - configure ports 27, 97, 103
 - FICON management style 105
 - configure Preferred Path 152
 - configure SNMP 27, 112
 - configure switch parameters 91
 - copy address configuration 111
 - define nickname 76
 - director properties 34, 58
 - displaying 59
 - enable feature key 114
 - export configuration report 29, 123
 - firmware library 31
 - FRU properties 34, 57
 - how to use 20
 - IPL 142
 - keyboard navigation 20
 - new feature key 114
 - node properties 76, 77
 - port binding 70
 - port card properties 61
 - port diagnostics 30
 - port properties 37, 64, 65, 76
 - save 126
 - save data collection 31
 - set online state 31
 - swap ports 30, 140
 - switch binding membership list 162
 - switchover CTP 62
 - switchover SBAR 62
 - unblock all ports 61, 68

- diamond, red
 - meaning of 43
 - port 64
- director
 - addressing, default values 147
 - audit log 127
 - date and time, configuring 115
 - element manager
 - messages 185
 - fibre channel addresses 92
 - FRU list view 84
 - identification, configuring 90
 - information, displaying 58
 - IP address
 - current 146
 - resetting configuration 146
 - IPL 59, 141
 - director menu 59
 - link incident log 87
 - node list view 75
 - NV-RAM 91, 95
 - offline state, setting 61
 - online state, setting 60
 - operating status 43
 - operation, monitoring 52
 - operational states 52, 142
 - performance view 79
 - priority, default value 147
 - rerouting delay 93
 - segmentation error 66
 - status bar, status indicator 53
 - status table 52
 - switch operating parameters 91
- Director 2/64 and 2/140 status bar, status indicator 53
- director element manager, description 16
- director menu 35, 59
- director properties dialog box 34
 - displaying 59
 - illustration 58
- discarded frames 82
- displaying port statistics 80
- DNS host name 90
- document
 - conventions 12
 - related documentation 11
- documentation, HP web site 11

- domain ID
 - director properties dialog box 58
 - insistent 92
 - preferred 92
- domain RSCNs 93
 - enterprise fabric mode 164

E

- e_d_tov 96
 - default value 147
 - fabric segmentation 96
 - less than r_a_tov 96
 - multiswitch fabrics 96
 - rerouting delay 93
- E_port segmentation
 - preferred domain ID 92
 - reasons, list of 66
- E_port segmentation errors, list of 66
- E_port, segmented, port state 87
- EBCDIC code pages 157
- element management
 - SNMP agent 16
- element manager
 - accessing 20
 - audit log 127
 - backing up and restoring 47
 - call-home notification, enabling 144
 - closing 44
 - configure 25
 - description 16
 - e-mail notification, enabling 143
 - FRU list view 42, 84
 - hardware view 33
 - help menu 32
 - identification, configuring the director 90
 - IPL 142
 - link incident log 87, 99
 - logs menu 29
 - maintenance menu 30
 - messages 185
 - node list view 38, 75
 - node list view menu 38
 - non-English language support 157
 - opening 20
 - overview 20
 - performance view 39, 79
 - performance view menu 40

- port list view 37, 72
 - menu 38
- port menu 35
- product 24
- status bar 42
- view panel 33
- window layout and function 23
- element menu 24
- e-mail notification
 - enabling 31, 143
 - LIN alerts 88, 99
- embedded port log 30, 135
- enable call-home notification option 31
- enable e-mail notification option 31
- enable feature key dialog box 114
- enable management server (FICON) 156
- enable telnet on director 29
- enable unit beaconing
 - product menu 25
- enable web server on director 29
- enabling
 - authorization traps 112
 - beaconing 69
 - call-home notification 144
 - e-mail notification 143
- engineering change level, director properties dialog box 58
- enterprise fabric mode 164
- error light, clearing 59
- error statistics 81
- ethernet connection, interrupted 141
- ethernet network DNS host name 90
- ethernet no-link status 52
- event codes, list of 129
- event data 130
- event log
 - capacity 125
 - illustration 128
 - using 128
- export configuration report
 - dialog box 29, 123
 - procedure 122
- extended distance buffering (10–100 km) 98
- extended distance, default value 147
- external loopback test 140

F

- fabric binding 159
 - enterprise fabric mode 164
 - online state functions 160
- fabric parameters
 - BB_Credit 95
 - descriptions 95
 - e_d_tov 96
 - interop mode 97
 - r_a_tov 95
 - switch priority 96
- fabric segmentation
 - e_d_tov 96
 - preferred domain ID 92
- factory defaults
 - configuration data 146
 - LIN alerts 99
- fan module
 - failure indicator 56
 - menu 35
- fault isolation, event log 128
- faults, event log 128
- feature key, configuring 113
- feature permissions 44
- features
 - Open Trunking 165
 - SANtegrity Binding 159
 - switch binding 160
- Fibre Channel address 75
 - node properties dialog box 78
 - port properties dialog box 65
- fibre channel addresses 92
- FICON management server 24, 91, 156
 - active=saved 156
 - code page 157
 - configuration procedure 157
 - configuring 113, 156, 157, 158
 - enable management server 156
 - host control 156
 - installing 156
 - parameters 156
 - programmed offline state control 156
- FICON management style 24, 94
 - addresses option 27
 - channel wrap test 70, 74
 - director options 60

- FICON management server [24](#), [91](#)
 - node properties [78](#)
 - port addresses, configuring [108](#)
 - port addressing [108](#)
 - port connection array [108](#)
 - port list view, addr column [72](#)
 - port swap [74](#)
 - ports
 - configuring [105](#)
 - swap ports [30](#), [70](#)
- file transfer protocol [140](#)
- firmware faults, event log [128](#)
- firmware level, director properties dialog box [58](#)
- firmware library dialog box [31](#)
- firmware versions [31](#)
 - managing [143](#)
- FPM card
 - beaconing, enabling [61](#)
 - LEDs [63](#)
 - loopback test [140](#)
 - port card view [63](#)
- frames
 - discarded [82](#)
 - performance view [83](#)
 - routing of [93](#)
- frames too long, error statistics [82](#)
- FRU
 - acronyms [84](#), [130](#)
 - description [25](#)
 - product menu [25](#)
- FRU list view [42](#), [84](#)
 - displaying [84](#)
 - illustration [42](#), [84](#)
 - menu [42](#)
- FRU properties [57](#)
 - cooling fan module [35](#)
 - CTP card [62](#)
 - dialog box [34](#), [57](#)
 - port card [61](#)
 - SBAR card [36](#), [62](#)
- FRUs
 - failures, event log [128](#)
 - position numbers [85](#)
- FTP [140](#)

G

- gateway address, default value [147](#)

H

HAFM

- configuring SNMP trap message recipients [111](#)
- messages [172](#)

HAFM appliance

- audit log [127](#)
- call-home feature [144](#)
- configuration, backing up and restoring [144](#)
- maintenance data [140](#)

- hardware failures, event log [128](#)

hardware log [29](#)

- capacity [125](#)
- detailed description [130](#)
- using [130](#)

hardware view [33](#), [51](#)

- component operation, monitoring [53](#)

CTP card

- menu [62](#)
- director information, displaying [58](#)
- director menu [59](#)
- director operation, monitoring [52](#)
- director status table [52](#)
- identifying FRUs [51](#)
- illustration [33](#), [54](#), [55](#)
- menu options, using [59](#)
- obtaining hardware status [56](#)
- online state [61](#)
- port card menu [61](#)
- port information, displaying [64](#)
- SBAR card menu [62](#)

help

- about option [32](#)
- contents option [32](#)

help menu [32](#)

- help, obtaining [13](#), [14](#)

- hop counts [93](#)

- host control [156](#)

- host control prohibited field [158](#), [159](#)

- host, audit log [127](#)

HP

- authorized reseller [13](#)
- storage web site [14](#)
- Subscriber's choice web site [13](#)
- technical support [13](#)

I

identification

- configuring for the director 90
- default values 147

illustrations 20

IML, CTP card 141

inactive state, reasons for 68

inactive, port state 86

inband director management

- FICON management style 24
- Open Systems management style 24

inband switch management 91

initial program load (IPL) 31

- executing 141

insistent domain ID 92

- enterprise fabric mode 165

internal loopback test 140

interop mode 97

invalid attachment, port state 86

invalid attachment, reasons for 67

invalid transmission words 82

IP address

- configuration, restoring 144
- default value 147

IPL 59

- connection interruption 141
- CTP card 141
- description 31
- dialog box 142
- executing 141

ISL

- load balancing 166

K

keyboard navigation in dialog boxes 20

L

languages, code page 157

laser LC transceiver 69

LEDs

- CTP card switchover 62
- FPM card 63
- port card view 63
- SBAR card switchover 62

light, signal, port state 86

LIN alerts configuration, port properties dialog box 66

LIN alerts, default values 147

link failures 81

link incident

- causes, list of 132
- port properties dialog box 66
- port state 86

link incident (LIN) alerts 87

- attention indicator 64
- clearing 70, 88
- configuring 99

link incident log 30, 87

- capacity 125, 132
- description 132
- illustration 132

link reset, port state 86

link resets, performance view 83

link utilization percentage, performance view 83

load balancing ISLs 166

logical port address 75

login

- password 15
- username 15

logs

- advanced
 - embedded port 30
 - embedded port log 135
 - switch fabric 30
 - switch fabric log 137

ASCII format 125

audit 29, 127

event 128

expanding columns 126

hardware 29, 130

link incident 30, 132

menu

- embedded port 30
- security 30
- switch fabric 30
- security 30
- window button function 125

logs menu 29

audit 29

hardware 29

link incident 30

loopback tests 68, 69, 140

loss of signal 132

loss of synchronization 132

M

MAC address, default 147

maintenance data, collecting 140

maintenance menu 30

 backup and restore configuration 32, 144

 collect maintenance data 140

 data collection 31

 enable call-home notification 31, 144

 enable e-mail notification 31, 143

 firmware library 31

 IPL 31, 141

 port diagnostics 30

 reset configuration 32, 146

 set online state 31, 142

 swap ports 30

maintenance port 146

management server

 FICON 156

 configuring 156

 installing 156

 Open Systems, installing 158

management style

 director properties dialog box 58

 FICON 91, 94

 Open Systems 91

 product menu 24

managing firmware versions 143

managing stored address configurations 110

matrix of port addresses 108

menu bar 24

menus

 configure 25

 CTP card 35, 62

 director 35, 59

 element 24

 fan module 35

 FRU list view 42

 hardware view 59

 help 32

 logs 29

 maintenance 30

 node list view 38, 76

 performance view 40, 79

 port 35, 61, 69

 port card 35

 port card view 36, 68

 port list 38

 port list view 74

 SBAR card 36, 62

messages

 element manager 185

 fabric manager 172

 HAFM application 172

mode

 enterprise fabric 164

 interop 97

 open fabric 1.0 97

model number, director properties dialog box 58

monitoring director operation 52

multiswitch fabric

 director, removing 142

 e_d_tov 96

 principal switch 96

 rerouting delay 93

N

N_ports, node list view 38

name, configure ports dialog box 97

new feature key dialog box 114

nickname

 port binding 100

 port binding error 67

nicknames, defining 76

nicknames, displaying 77

no light, port state 86

node list view 38, 75

 addr column 75

 illustration 39, 75

 menu 38, 76

 port # column 75

 port wwn column 75

 unit type column 75

node nickname, node properties dialog box 78

node properties dialog box 76, 77

 displaying 69

 illustration 77

node properties, displaying 38, 76

node WWN, port properties dialog box 78

no-link status 52

NOS

- hardware log [132](#)
- port state [86](#)
- not installed, port state [87](#)
- not operational, port state [86](#)
- not-operational (NOS) primitive sequence, hardware log [132](#)

NV-RAM

- configuring [91](#)
- export configuration report [122](#)
- fabric parameters and [95](#)

O

offline sequences (OLS)

- FICON management style [109](#)
- performance view [83](#)

offline signals (OLS) [69](#)

offline state, setting [61](#)

offline, port state [87](#)

OLS [98](#)

- FICON management style [109](#)

online state, setting [60](#), [142](#)

online, port state [86](#)

open element manager [20](#)

open fabric 1.0 [97](#)

open port card view [61](#)

Open Systems Management Server

- configuring [113](#), [159](#)
- installing [158](#)
- option [27](#)

Open Systems management server [24](#)

Open Systems management style [24](#), [91](#)

- configuring ports [103](#)
- node properties [78](#)

Open Trunking

- description [165](#)
- enabling and configuring [166](#)

Open Trunking feature

- dialog box [166](#)
- dialog box menu [168](#)

operating parameters [26](#)

- default values [147](#)

operating speed, port properties dialog box [65](#)

operating status for the director [43](#)

operational state, port properties dialog box [66](#)

operational states for ports [86](#)

operational states, port [73](#)

P

part number, hardware log [131](#)

password, default [15](#)

performance view [39](#), [79](#)

- bar graph [80](#)
- button functions [84](#)
- illustration [79](#)
- menu [79](#)

- port, statistics [80](#)

performance view menu [40](#)

periodic synchronization, date and time, configuring [115](#)

permissions for feature functions [44](#)

port addresses

- default value [147](#)
- FICON management style [108](#)
- matrix of [108](#)
- node properties dialog box [78](#)

port binding

- description [70](#)
- enabling [100](#)

port binding dialog box [70](#)

port binding error [67](#)

port binding feature

- bound WWN [100](#)
- configuring ports [97](#)

port blocked states, default value [147](#)

port card

- acronyms, port technology [85](#)
- attention indicator [55](#)
- failure indicator [55](#)
- properties [61](#)
- status, determining [36](#)

port card properties dialog box [61](#)

port card view

- displaying [61](#), [63](#)
- illustration [36](#), [63](#)
- opening [61](#)

port card view menu [35](#), [36](#), [68](#)

port configuration data, NV-RAM storage [97](#)

port connection array, FICON management style [108](#)

port diagnostics

- external loopback test [140](#)
- internal loopback test [140](#)

- port diagnostics dialog box 30
 - displaying 69
 - displaying from port card menu 61, 68
 - displaying from port menu 69
- port failure, port state 87
- port list view 37, 72
 - displaying 37, 72
 - illustration 37, 72
 - menu 74
- port list view menu 38
- port menu 35, 61, 69
- port name
 - configure ports dialog box 97
 - FICON management style 108, 110
 - port properties dialog box 65
- port nickname, port properties dialog box 78
- port number
 - configure ports dialog box 97
 - node properties dialog box 77
 - port properties dialog box 65
- port operational states 73
 - table of 86
- port optics 64, 86
- port pop-up menu 35
- port properties dialog box 65, 76
 - displaying 37, 69, 73
- port properties, displaying 76
- port statistics
 - class 2 statistics 81
 - class 3 statistics 81
 - error statistics table 81
 - traffic statistics 83
- port technology dialog box, displaying 69
- port transmission, blocking 69
- port type 100
- port WWN 75
 - node properties dialog box 78
- port wwn 75
- ports
 - address 72, 75
 - bar graph 39, 80
 - binding 70
 - blocked states 72
 - blocking 98
 - FICON management style 108, 109
 - blocking all 61, 68
 - channel wrap test 74
 - configuring 27, 97
 - FICON management style 105
 - Open Systems management style 103
 - connections, prohibiting 108
 - counters, clearing 41, 44
 - default configuration 27
 - default values 147
 - description 24
 - diagnostics 30, 68
 - menu option 61
 - displaying information 64
 - displaying statistics 41
 - event log 128
 - extended distance buffering (10–100 km) 98
 - failed, status symbol 64
 - FICON management style 27
 - loopback tests 68, 69
 - maintenance 146
 - naming 97
 - Open Systems management style 27
 - operating speed 65
 - operating states 63
 - operational states, table of 86
 - product menu 24
 - resetting 70
 - speed 69
 - statistics
 - description 80
 - displaying 80
 - status, determining 36
 - swapping 30, 74
 - transmission, blocking 69
 - type 73
 - port properties dialog box 65
 - UDP, default value 148
 - unblocking 61
 - WWN 65
- power indicator 56
- power supply, failure indicator 56
- preferred domain ID 92
 - default value 147
 - multi-switch fabric 92
- Preferred Path
 - description 150
 - dialog box 152
- Preferred Path feature 26, 150

- primitive sequence
 - errors [82](#)
 - hardware log [132](#)
- principal switch, determining [96](#)
- problems, event log [128](#)
- product menu
 - clear system error light [25](#)
 - close [25](#)
 - enable unit beaconing [25](#)
 - FRU [25](#)
 - management style [24](#)
 - port [24](#)
 - ports [24](#)
 - properties [25](#)
- programmed offline state control [156](#)
- properties
 - product menu [25](#)

R

- r_a_tov [95](#)
 - default value [147](#)
 - greater than e_d_tov [96](#)
 - synchronization, loss of [132](#)
- rack stability, warning [13](#)
- reason field [52](#)
 - port properties dialog box [66](#)
- receive values [83](#)
- related documentation [11](#)
- remote user workstations [17](#)
- rerouting delay [93](#)
 - enterprise fabric mode [164](#)
- reset configuration option [32](#)
- reset port option [70](#)
- resetting
 - configuration [146](#)
 - configuration data [146](#)
- routing delay, default value [147](#)
- RSCNs
 - domain [93](#)
 - suppress [94](#)
- RX BB Credit, configuring [98](#)

S

- SANtegrity Binding
 - description [159](#)
 - switch binding [160](#)

- SANtegrity Binding feature
 - fabric binding [159](#)
- save data collection dialog box [31](#)
- save dialog box [126](#)
- SBAR card
 - beaconing indicator [56](#)
 - beaconing, enabling [62](#)
 - failure indicator [56](#)
 - FRU properties [62](#)
 - switchover [62](#)
- SBAR card menu [36, 62](#)
- security log [30](#)
- segmentation, reasons for error [66](#)
- segmented E_port, port state [87](#)
- sequence errors [82](#)
- serial number
 - hardware log [131](#)
- set director date and time manually [116](#)
- set online state dialog box [31](#)
- setting online state [142](#)
- severity classifications [129](#)
- signal light, port state [86](#)
- signal losses, error statistics [82](#)
- signal, loss of [132](#)
- simple network management protocol, see SNMP
- SMTP server address [31](#)
- SNMP agent option [16, 27](#)
- SNMP authorization trap states, default value [148](#)
- SNMP communities, default value [148](#)
- SNMP default values [148](#)
- SNMP management station, audit log [127](#)
- SNMP write authorizations, default value [148](#)
- speeds
 - port [65, 69](#)
 - UPM cards [94](#)
- square, gray, meaning of [43](#)
- statistics values tables [80](#)
- statistics, ports [41, 80](#)
- status bar [42, 43, 53](#)
- status bar symbols [43](#)
- status field [52](#)
- status indicator [53](#)
- status symbols [53](#)
- StorageWorks director 2/64
 - audit log [127](#)
 - IPL [141](#)
 - operational states [142](#)

- stored address configurations, managing 110
- stored addresses 27
- subnet mask, default value 147
- Subscriber's choice, HP 13
- support center server 144
- suppress RSCNs 94
- swap ports dialog box 30, 140
- swapping ports 70, 74
- switch binding 160, 164
 - configuring 97
 - enable and disable 161
 - membership list 162
 - online state functions 163
 - zoning function 163
- switch binding membership list dialog box 162
- switch clock alert mode 156
 - date and time, configuring 115
- switch clock alert mode field 158
- switch fabric log 30, 137
- switch operating parameters
 - configuring for the director 91
- switch parameters
 - descriptions 92
 - domain RSCNs 93
 - insistent domain ID 92
 - NV-RAM storage 91, 95
 - preferred domain ID 92
 - rerouting delay 93
 - suppress RSCNs 94
- switch priority
 - description 96
 - related number codes 97
- switch priority setting 96
- switches, principal, determining 96
- switchover CTP dialog box 62
- switchover SBAR card 62
- switchover SBAR dialog box 62
- symbols
 - in text 12
 - status bar, table of 43
- sync losses 82
- synchronization, loss of 132
- synchronize date and time 116
- system error
 - indicator 56
 - light, clearing 59

T

- technical support 140
- technical support, HP 13
- testing, port state 87
- text symbols 12
- threshold alerts 28
 - clearing 71
 - configuring 117
 - general information 88
 - port properties dialog box 68
- traffic statistics 83
- transmission words, invalid 82
- transmit values 83
- trap recipient IP addresses, default value 148
- traps, SNMP 111
- triangle, yellow
 - LIN alert 99
 - meaning of 43
- triangle, yellow, port connector 64
- trunking feature
 - dialog box 166
 - dialog box menu 168
 - enabling and configuring 166

U

- UDP port, default value 148
- unblock all ports dialog box, displaying 61, 68
- unit beaconing, enabling 59
- unit type 75
- unit type, node properties dialog box 78
- United States/Canada 00037 code page 157
- universal port module cards 94
- UPM cards 94
- username, default 15

V

- versions, firmware 31
 - managing 143
- view menu
 - port list 72
- view panel 33
- view tabs 33

views

- FRU list [84](#)
- hardware [51](#)
- node list [75](#)
- performance [79](#)
- port list [72](#)

W

warning

- rack stability [13](#)

warnings

- resetting configurations [32](#)

web server, enabling [29](#)

web sites

- HP documentation [11](#)
- HP storage [14](#)
- HP Subscriber's choice [13](#)

window layout [23](#)

Windows dial-up networking [144](#)

WWN

- director properties dialog box [58](#)
- format [70](#)
- nickname for [77](#)
- node list view [75](#)
- port binding [100](#)
- port binding error [67](#)
- port properties dialog box [65](#)
- principal switch [96](#)

Z

zone members, default value [148](#)

zone set state, default value [148](#)

zone sets, default value [148](#)

zone states, default value [148](#)

zones, number of, default value [148](#)

zoning

- configuration, backing up and restoring [145](#)
- default values [148](#)

